

(11)Publication number : 11-177582

(43)Date of publication of application : 02.07.1999

(51)Int.Cl.

H04L 12/28
G09C 1/00
G09C 1/00
H04L 9/32
H04L 12/66
H04L 12/56

(21)Application number : 10-227337

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 11.08.1998

(72)Inventor : ICHIKAWA TAKEO
KAYAMA HIDETOSHI
YAMAMOTO HIROYUKI
TAKANASHI HITOSHI
MORIKURA MASAHIRO

(30)Priority

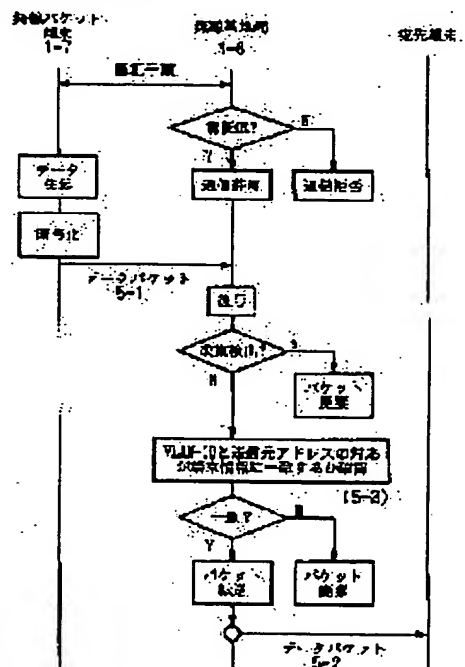
Priority number : 09228966 Priority date : 12.08.1997 Priority country : JP

(54) PACKET TRANSFER METHOD AND BASE STATION USED FOR THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To permit only a terminal that is previously registered to transfer the packets to a specific data network by ciphering the data to be transmitted via an authenticated packet terminal, decoding the ciphered data on a received packet via a packet network and permitting the communication of the data as long as they are not altered.

SOLUTION: A radio base station 1-6 authenticates a radio packet terminal 1-7 when the communication is started and then starts the communication if the terminal 1-7 is the normal one. When the alteration of a data packet 5-1 of the terminal 1-7 is detected, the packet 5-1 is disused. When no alteration of the packet 5-1 is detected, a terminal address/VLAN-ID comparison means of the station 1-6 refers to the terminal information stored in a terminal information storage means to confirm the correspondence between the VLAN-ID and the transmitter address. Based on this confirmation result, a data packet 5-2 is transferred to the destination terminal that is designated by a destination address as long as the correspondence is coincident with the terminal information.



LEGAL STATUS

[Date of request for examination] 28.12.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3009876

[Date of registration] 03.12.1999

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

特開平 1 1 - 1 7 7 5 8 2

(43) 公開日 平成 1 1 年 (1 9 9 9) 7 月 2 日

(51) Int. Cl.	識別記号	庁内整理番号	F I	技術表示箇所	
H04L 12/28			H04L 11/00	310	B
G09C 1/00	640		G09C 1/00	640	D
				640	E
	660			660	E
H04L 9/32			H04L 9/00	673	B

審査請求 有 請求項の数 1 5 O L (全 3 4 頁) 最終頁に続く

(21) 出願番号 特願平 1 0 - 2 2 7 3 3 7

(22) 出願日 平成 1 0 年 (1 9 9 8) 8 月 1 1 日

(31) 優先権主張番号 特願平 9 - 2 2 8 9 6 6

(32) 優先日 平 9 (1 9 9 7) 8 月 1 2 日

(33) 優先権主張国 日本 (J P)

(71) 出願人 0 0 0 0 0 4 2 2 6

日本電信電話株式会社

東京都新宿区西新宿三丁目 1 9 番 2 号

(72) 発明者 市川 武男

東京都新宿区西新宿三丁目 1 9 番 2 号 日

本電信電話株式会社内

(72) 発明者 加山 英俊

東京都新宿区西新宿三丁目 1 9 番 2 号 日

本電信電話株式会社内

(72) 発明者 山本 浩之

東京都新宿区西新宿三丁目 1 9 番 2 号 日

本電信電話株式会社内

(74) 代理人 弁理士 志賀 正武

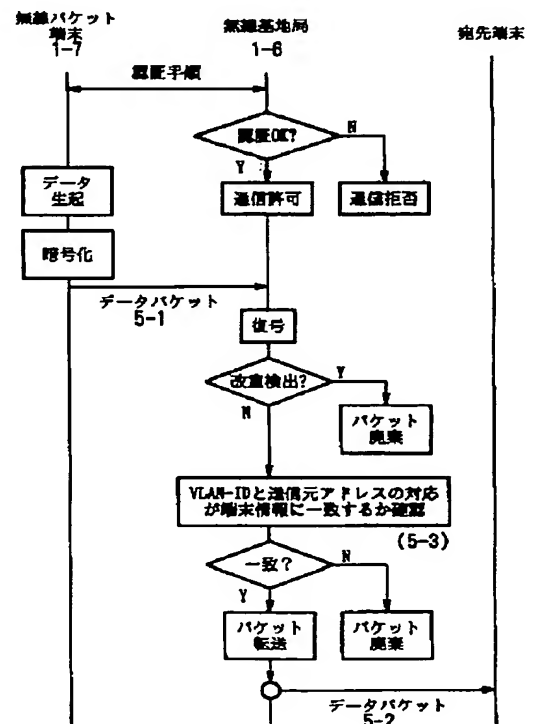
最終頁に続く

(54) 【発明の名称】 パケット転送方法および該方法に用いる基地局

(57) 【要約】

【課題】 送信元アドレスの偽造によりユーザ LAN へ不正にアクセスできる問題を解決し、予め登録した端末のみ特定のユーザ LAN とのパケット転送だけを許可するパケット転送方法を提供する。

【解決手段】 ユーザ LAN を識別する VLAN-ID を定義しておき、無線パケット網は端末アドレスと VLAN-ID と端末認証に必要な情報を対応づけた端末情報を予め記憶し、通信開始時においてまず無線パケット端末の認証を行う。次に無線パケット端末は自身が属するユーザ LAN の VLAN-ID を付与した暗号化パケットを送信し、無線パケット網は暗号の復号時に改竄を調べ、改竄がない場合は送信元アドレスと VLAN-ID の対応を確認し、端末情報と一致する場合は宛先アドレスに転送する。端末認証の結果が不正端末であった場合、復号時に改竄がある場合、送信元アドレスと VLAN-ID の対応が端末情報に不一致している場合はパケットを廃棄する。



【特許請求の範囲】

【請求項 1】 パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザ LAN に接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、

前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に前記パケット端末の端末認証を行い、

認証に成功した前記パケット端末は、送信すべきデータを暗号化して、前記宛先端末が属するユーザ LAN に割り当てられる識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、

前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データを復号し、該受信パケットが改竄されていないならば、前記受信パケットに含まれる前記送信元アドレス及び前記識別子に基づいて、該識別子を持つユーザ LAN に対して前記パケット端末が通信を許可されている場合にだけ前記受信パケットを該ユーザ LAN に転送し、該通信が許可されていない場合には前記受信パケットを廃棄することを特徴とするパケット転送方法。

【請求項 2】 パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザ LAN に接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、

前記ユーザ LAN を識別する識別子を前記各ユーザ LAN にあらかじめ割り当てておき、

前記パケット網は、前記端末アドレスと通信を許されている 1 つ以上のユーザ LAN にそれぞれ割り当てられた前記識別子と端末認証に必要な情報とを対応づけた端末情報をあらかじめ記憶し、

前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば前記パケット端末に対して通信許可を通知

し、

前記パケット端末は、前記通信許可が通知されたのであれば、1 つ以上の前記ユーザ LAN の中から通信するユーザ LAN を一つ選択し、送信すべきデータを暗号化して、該選択したユーザ LAN に割り当てられた識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、

前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には、前記受信パケットに含まれる前記送信元アドレスと前記識別子との対応が前記端末情報に登録されているかどうかを確認し、該対応が登録済みである場合には前記受信パケットを前記宛先アドレスに転送し、該対応が未登録の場合には前記受信パケットを廃棄することを特徴とするパケット転送方法。

【請求項 3】 パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザ LAN に接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、

前記ユーザ LAN 毎にあらかじめ固有のユーザ LAN 名を割り当てておき、

前記パケット網は、前記端末アドレスと通信を許されている 1 つ以上のユーザ LAN にそれぞれ割り当てられた前記ユーザ LAN 名と端末認証に必要な情報を対応づけた端末情報をあらかじめ記憶し、

前記パケット端末は前記基地局を介して通信を開始する際に、1 つ以上の前記ユーザ LAN の中から通信するユーザ LAN を一つ選択し、該選択したユーザ LAN に割り当てられた前記ユーザ LAN 名を前記パケット網へ通知し、

前記パケット網は、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば、前記パケット端末から通知された前記ユーザ LAN 名に対して前記ユーザ LAN を識別するための識別子を割り当てて前記パケット端末に通知し、

前記パケット端末は、送信すべきデータを暗号化して、前記選択したユーザ LAN に割り当てられた識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、

前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無

を判定し、改竄が検出されていれば前記受信バケットを廃棄し、改竄されていない場合には、前記受信バケットに含まれる識別子を割り当てたユーザ LAN 名と前記受信バケットに含まれる送信元アドレスとの対応が前記端末情報に登録されているかどうかを確認し、該対応が登録済みである場合には前記受信バケットを前記宛先アドレスに転送し、該対応が未登録の場合には前記受信バケットを廃棄し、

前記バケット網は、その後に前記バケット端末が通信を終了した時に前記ユーザ LAN 名に割り当てた前記識別子を解放するようにしたことを特徴とするバケット転送方法。

【請求項 4】 前記バケットバックボーン網が、前記バケットを中継する複数の中継ノードを有し、これら各中継ノードが前記受信バケットを前記宛先アドレスに転送するための経路選択の機能を有するネットワークを用いたバケット転送方法であって、

前記バケット網は、前記経路選択のためのルーティング情報として前記受信バケット中の前記宛先アドレスと前記識別子とを用い、

ユニキャストバケットを転送する場合、前記宛先端末が前記バケット網に接続中であれば、前記宛先アドレスに応じて前記中継ノードを順次選択しながら該バケットを前記宛先端末まで転送し、前記宛先端末が前記バケット網に接続中でなければ、前記識別子に応じて前記中継ノードを順次選択しながら該バケットを前記ユーザ LAN まで転送し、

ブロードキャストバケット及びマルチキャストバケットを転送する場合は、前記識別子を用いて前記中継ノードを順次選択して該中継ノードに該バケットを順次転送してゆき、同じ識別子を用いて通信中の全ての前記バケット端末及び該識別子により指定される前記ユーザ LAN に該バケットを転送することを特徴とする請求項 2 記載のバケット転送方法。

【請求項 5】 前記バケットバックボーン網と前記複数のユーザ LAN の間をゲートウェイで接続したネットワークを用いたバケット転送方法であって、

前記ユーザ LAN を介して前記受信バケットを前記宛先アドレスへ転送する際、前記ゲートウェイが前記受信バケットに含まれる前記識別子に応じて前記ユーザ LAN を選択して該選択されたユーザ LAN へ前記受信バケットを転送することを特徴とする請求項 2 ～ 4 の何れかの項記載のバケット転送方法。

【請求項 6】 バケット網が基地局と該基地局を接続するバケットバックボーン網とから構成されており、前記基地局が配下に複数のバケット端末を収容しており、前記バケットバックボーン網がさらに複数の他バケット網であるユーザ LAN にゲートウェイを介して接続されているネットワークを用いたバケット通信であり、前記各バケット端末は固有の端末アドレスを有すると共に宛先

端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したバケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記バケットの転送を行うバケット転送方法であって、

前記バケット網は、前記端末アドレスと端末認証に必要な情報とを対応づけた端末情報をあらかじめ記憶し、

前記ゲートウェイは、前記バケット網と前記ユーザ LAN の間でバケットの転送を許可する送信元の端末アドレスをあらかじめ記憶し、

前記バケット網は、前記バケット端末が前記基地局を介して通信を開始する際に、前記情報を使用して前記バケット端末の端末認証を行い、前記バケット端末が正規の端末であれば前記バケット端末に通信許可を通知し、前記バケット端末は、前記通信許可が通知されたのであれば、送信すべきデータを暗号化して前記宛先アドレスと前記送信元アドレスを付与したバケットを前記バケット網へ送信し、

前記バケット網は、前記バケットを受信して該受信バケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信バケットを廃棄し、改竄されていない場合には前記受信バケットを前記ゲートウェイに転送し、

前記ゲートウェイは、前記バケット網から転送されたバケットに含まれる前記送信元アドレスに対する転送が許可されている場合は該転送バケットを前記ユーザ LAN から前記宛先アドレスに転送し、該転送が許可されていない場合は該転送バケットを廃棄するようにしたことを特徴とするバケット転送方法。

【請求項 7】 前記バケットバックボーン網が、前記バケットを中継する複数の中継ノードを有し、これら各中継ノードが前記バケットを前記宛先アドレスに転送するための経路選択機能を有するネットワークを用いたバケット転送方法であって、

前記ユーザ LAN を識別する識別子を前記各ユーザ LAN にあらかじめ割り当てておき、

前記バケット網は、前記バケットを前記バケット網へ送信する際に、複数の前記ユーザ LAN の中から接続するユーザ LAN を一つ選択して、該選択したユーザ LAN の識別子を前記バケットにさらに付与して送信し、

前記バケット網は、前記経路選択のためのルーティング情報として送信された前記バケットに含まれる前記宛先アドレスと前記識別子とを用い、

ユニキャストバケットを転送する場合、前記宛先端末が前記バケット網に接続中であれば、前記宛先アドレスに応じて前記中継ノードを順次選択しながら該バケットを前記宛先端末まで転送し、前記宛先端末が前記バケット網に接続中でなければ、前記識別子に応じて前記中継ノードを順次選択しながら該バケットを前記ゲートウェイに転送し、

ブロードキャストパケット及びマルチキャストパケットを転送する場合は、前記識別子を用いて前記中継ノードを順次選択して該中継ノードに該パケットを順次転送してゆき、同じ識別子を用いて通信中の全ての前記パケット端末と、該識別子により指定される前記ゲートウェイとに転送することを特徴とする請求項 6 記載のパケット転送方法。

【請求項 8】 前記暗号化及び前記復号化に際し、前記ユニキャストパケットを転送する場合は、前記各パケット端末毎に割り当てた暗号鍵を用い、前記ブロードキャストパケット又は前記マルチキャストパケットを転送する場合は、前記各識別子毎に割り当てた暗号鍵を用いることを特徴とする請求項 4 又は 7 記載のパケット転送方法。

【請求項 9】 前記暗号化及び前記復号化に際し、前記ユニキャストパケットを転送する場合及び前記パケット端末が前記ブロードキャストパケット又は前記マルチキャストパケットを送信する場合は、前記各パケット端末毎に割り当てた暗号鍵を用い、前記基地局が前記ブロードキャストパケット又は前記マルチキャストパケットを送信する場合は、前記各識別子毎に割り当てた暗号鍵を用いることを特徴とする請求項 4 又は 7 記載のパケット転送方法。

【請求項 10】 前記暗号化及び前記復号化に際し、暗号鍵として前記各識別子毎に割り当てた暗号鍵を用いることを特徴とする請求項 4 又は 7 記載のパケット転送方法。

【請求項 11】 他パケット網であるユーザ LAN が複数接続されたパケットバックボーン網に接続され、かつ、配下に複数のパケット端末を収容する基地局であって、

前記各パケット端末に付与された固有の端末アドレスと、前記パケット端末が通信を許されている 1 つ以上のユーザ LAN にそれぞれ割り当てられた識別子と、端末認証に必要な情報を対応づけて記憶する端末情報記憶手段と、

前記パケット端末からの通信開始要求に応じて前記情報を使用した端末認証を行い、前記パケット端末に対して認証結果を通知する端末認証手段と、

前記パケットバックボーン網と前記パケット端末の間で授受されるパケット中のデータ部を前記情報を用いて暗号化して送信するパケット暗号化手段と、

宛先端末の前記端末アドレスである宛先アドレスと前記パケット端末の端末アドレスである送信元アドレスと前記ユーザ LAN に割り当てられた識別子が暗号化データに付与されたパケットを前記パケット端末から受信して該暗号化データを復号するパケット復号化手段と、

前記復号されたデータから改竄を検出して該パケットを廃棄するパケット改竄検出手段と、

前記パケットに含まれている前記送信元アドレス及び前

記識別子の組が、前記端末情報記憶手段に記憶されている前記端末アドレス及び前記識別子の組の中に登録されているかどうかを確認する比較手段と、

前記比較手段による確認結果に基づいて、前記登録があることを条件に前記宛先アドレスに前記パケットを転送し、前記登録が無いことを条件に前記パケットを廃棄するフィルタリング手段とを具備することを特徴とする基地局。

【請求項 12】 他パケット網であるユーザ LAN が複数接続されたパケットバックボーン網に接続され、かつ、配下に複数のパケット端末を収容する基地局であって、

前記各パケット端末に付与された固有の端末アドレスと、前記パケット端末が通信を許されている 1 つ以上のユーザ LAN にそれぞれ割り当てられたユーザ LAN 名と、端末認証に必要な情報を対応づけて記憶する端末情報記憶手段と、

前記パケット端末からの通信開始要求に応じて前記情報を使用した端末認証を行って、認証結果を前記パケット端末に通知するとともに、正規のパケット端末に対しては、前記通信開始要求に伴って前記パケット端末から通知されるユーザ LAN 名に前記ユーザ LAN を識別するための識別子を割り当てて通知し、前記パケット端末が通信を終了したことを条件として前記ユーザ LAN 名に割り当てた前記識別子を解放する端末認証手段と、

前記パケットバックボーン網と前記パケット端末の間で授受されるパケット中のデータ部を前記情報を用いて暗号化して送信するパケット暗号化手段と、

宛先端末の前記端末アドレスである宛先アドレスと前記パケット端末の端末アドレスである送信元アドレスと前記識別子が暗号化データに付与されたパケットを前記パケット端末から受信して該暗号化データを復号するパケット復号化手段と、

前記復号されたデータから改竄を検出して該パケットを廃棄するパケット改竄検出手段と、

前記受信したパケットに含まれる識別子を割り当てたユーザ LAN 名と前記受信したパケットに含まれる送信元アドレスの組が、前記端末情報記憶手段に記憶されている前記ユーザ LAN 名及び前記端末アドレスの組の中に登録されているかどうかを確認する比較手段と、

前記比較手段による確認結果に基づいて、前記登録があることを条件に前記宛先アドレスに前記パケットを転送し、前記登録が無いことを条件に前記パケットを廃棄するフィルタリング手段とを具備することを特徴とする基地局。

【請求項 13】 前記パケット暗号化手段は、送信するパケットがユニキャストパケットであれば、各パケット端末毎に割り当てた暗号鍵を用いて暗号化し、前記送信するパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた

暗号鍵を用いて暗号化し、

前記パケット復号化手段は、受信したパケットがユニキャストパケットであれば、前記各パケット端末毎に割り当てた暗号鍵を用いて復号化し、前記受信したパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて復号化することを特徴とする請求項 1 1 記載の基地局。

【請求項 1 4】 前記パケット暗号化手段は、送信するパケットがユニキャストパケットであれば、各パケット端末毎に割り当てた暗号鍵を用いて暗号化し、前記送信するパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて暗号化し、

前記パケット復号化手段は、前記各パケット端末毎に割り当てた暗号鍵を用いて復号化することを特徴とする請求項 1 1 記載の基地局。

【請求項 1 5】 前記パケット暗号化手段は、前記各識別子毎に割り当てた暗号鍵を用いて送信するパケットのデータ部を暗号化し、

前記パケット復号化手段は、前記各識別子毎に割り当てた暗号鍵を用いて受信したパケットのデータ部を復号化することを特徴とする請求項 1 1 記載の基地局。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】本発明は、無線または有線のパケット通信におけるパケット転送方法および該方法に用いる基地局に関する。さらに詳しくは、コネクションレス型のデータ通信において、パケット網に複数の L A N (Local Area Network; ローカルエリアネットワーク) を接続して仮想 L A N (V L A N) を構成したネットワークにおけるパケット転送方法および該方法に用いる基地局に関するものである。

【 0 0 0 2 】

【従来の技術】インターネットでは、I P (Internet Protocol; インターネットプロトコル) がパケット転送方法に採用され、このため各端末は I P アドレスを有する。I P アドレスは 3 2 b i t で構成され、上位ビットの一部はデータ網を識別するためのネットワークアドレスを示し、残りの下位ビットはデータ網に接続する端末を識別するためのホストアドレスを示す。

【 0 0 0 3 】 端末は、データ宛先アドレスと送信元アドレスを付与したパケットを I P ネットワークに送信し、I P ネットワークは宛先アドレス中のネットワークアドレスで示されるデータ網にパケットを転送する。データ網は、パケットがユニキャストパケットの場合は宛先アドレス中のホストアドレスで指定された端末に転送し、パケットがブロードキャストパケットの場合はデータ網に接続する全ての端末に転送する (R F C 7 9 1 I n t e r n e t Protocol)。

【 0 0 0 4 】 かししながら、このようなパケット転送方法によると、送信元の端末が何者であるかを確認せずにデータ網へパケットを転送するため、未知の端末によりデータ網が不正にアクセスされる危険性がある。また、たとえ送信元端末が正規の端末であったとしても、宛先アドレスを規制していないことから、送信元端末が属するデータ網以外の他のデータ網への不正アクセスを防止できないという問題もある。

【 0 0 0 5 】 このような不都合を解消するために、パケット転送時に宛先アドレスと送信元アドレスをチェックするパケット転送方法が提案されている。

【 0 0 0 6 】 このアドレスチェック方法では、転送を許可する宛先アドレスと送信元アドレスとの組合せをあらかじめ許可テーブルとしてパケット転送装置に登録しておく。パケット転送装置は、転送パケットの宛先アドレスと送信元アドレスをチェックして、これらアドレスが許可テーブルに登録済みの場合は転送パケットを転送し、未登録の場合は転送パケットを転送しない (石坂隆宏、「ネットワーク・セキュリティ装置」、特開平 2 - 3 0 2 1 3 9 号公報)。

【 0 0 0 7 】 この方法によれば、送信元アドレスを確認して、あらかじめ許可した端末アドレスの時にだけパケットを転送することにより、データ網への不正アクセスを防止している。しかし、この方法では送信元アドレスを偽造することによってデータ網へ不正にアクセスできるという問題が生じる。

【 0 0 0 8 】 従来の他のパケット転送方法として強制転送と呼ばれる方法が提案されている。この方法は、コネクションオリエンテッド型のパケット網 (即ち、X. 2 5 に代表され、通信を開始する際にコネクションを設定するパケット網) に複数のデータ網が接続しているとき、パケット網を通してアクセスしようとする呼をパケット網がセキュリティチェック用のデータベースマシンに強制転送する。そして、データベースマシンがアクセスの正当性をチェックして、正当な場合はアクセス呼をデータ網に転送して端末-データ網間にコネクションを設定し、不当な場合はアクセス呼を切断するものである (大吉 章次、「パケット交換網におけるセキュリティチェック方式」、特開平 5 - 3 2 7 7 7 3 号公報)。

【 0 0 0 9 】 かししながら、この方法では、パケットに付与された宛先アドレスにより転送を行うコネクションレス型のパケット網に適用した場合、セキュリティチェック用のデータベースマシンに全ての転送パケットを強制転送してアクセスの正当性をチェックする必要がある。そのために、セキュリティチェック用のデータベースマシンの負荷の増加とパケット転送遅延時間の増加という問題が生じる。

【 0 0 1 0 】 さらに、従来の他のパケット転送方法として、不特定多数の端末が接続するインターネット等のネットワーク (以下、「中継ネットワーク」という) を経

由して、リモート端末がデータ網にアクセスすることを可能にしつつ、データ網への不正アクセスを防止するカプセル化方法が提案されている。この方法では、データ網がゲートウェイを介して中継ネットワークに接続する。ゲートウェイは通信開始時にまずリモート端末の認証を行い、不正端末であることが判明した場合はパケットを破棄する。次に、リモート端末は、宛先アドレスと送信元アドレスが含まれた送信パケットを暗号化してゲートウェイへ送信する。この時、暗号化された送信パケットは、ゲートウェイ宛のパケットのデータ部に格納され、宛先データ網に接続されたゲートウェイのアドレスと送信元アドレスが付加されて中継ネットワークに転送される。なおこのようにしてパケットを転送することをカプセル化と呼んでいる。ゲートウェイは受信パケットからデータ部を取り出して暗号化されたパケットを復号する。この復号時に改竄を検出した場合はパケットを破棄し、改竄されていない場合はパケットをデータ網へ転送する。一方、データ網からリモート端末に宛てたパケットは、送信元のデータ網に接続されたゲートウェイが、宛先アドレスと送信元アドレスを付加して暗号化したのち、これに宛先アドレスと自分のゲートウェイアドレスをさらに付加し、カプセル化してリモート端末に転送する。

【0011】この方法によれば、リモート端末を認証した後、ゲートウェイとリモート端末間にカプセル化による暗号路を設定してデータ網への不正アクセスを防止している。しかしながら、リモート端末が、中継ネットワーク経由で接続している他のリモート端末にパケットを送信する場合には、必ずゲートウェイを経由して転送されるため、最適な経路選択が行われず、パケット転送遅延時間が増加するという問題が生じる。また、ゲートウェイは、自身に接続しているデータ網に属する全ての端末についてカプセル化／デカプセル化処理を行う必要があり、ゲートウェイの処理負荷が増大してしまう。また、この方法では、データ網またはリモート端末がブロードキャストパケットやマルチキャストパケットを転送する場合に、中継ネットワークに送られるパケットの宛先アドレスにブロードキャストアドレスやマルチキャストアドレスを指定することができない。そのため、ゲートウェイはパケットを複製してから各リモート端末にユニキャスト転送するしかなく、中継ネットワークのトラフィック増加とパケット転送遅延時間の増加という問題が生じるほか、ゲートウェイの負荷が増大するという問題も生じる。さらに、送信元リモート端末から宛先リモート端末へユニキャストパケットを転送する場合、たとえこれらリモート端末が中継ネットワークに接続していても、必ず当該データ網に接続しているゲートウェイを経由してから宛先端末にパケットが送られるため、転送遅延時間が増加するという問題を生じる。

【0012】

【発明が解決しようとする課題】従って本発明の第1の目的は、送信元アドレスを偽造することによりユーザLANへ不正にアクセスできてしまう問題を解決し、あらかじめ登録した端末に対してだけ特定のデータ網とのパケット転送を許可するパケット転送方法および該方法に用いる基地局を提供することにある。

【0013】また、本発明の第2の目的は、パケットの転送遅延時間、トラフィック、ゲートウェイの負荷が増加する問題点を解決し、最適な経路選択が可能でなおかつ効率的なパケット転送方法および該方法に用いる基地局を提供することにある。

【0014】

【課題を解決するための手段】以上の課題を解決するために、請求項1記載の発明は、パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザLANに接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に前記パケット端末の端末認証を行い、認証に成功した前記パケット端末は、送信すべきデータを暗号化して、前記宛先端末が属するユーザLANに割り当てられる識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データを復号し、該受信パケットが改竄されていなければ、前記受信パケットに含まれる前記送信元アドレス及び前記識別子に基づいて、該識別子を持つユーザLANに対して前記パケット端末が通信を許可されている場合にだけ前記受信パケットを該ユーザLANに転送し、該通信が許可されていない場合には前記受信パケットを廃棄することを特徴としている。

【0015】また、請求項2記載の発明は、パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザLANに接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法で

あって、前記ユーザ LAN を識別する識別子を前記各ユーザ LAN にあらかじめ割り当てておき、前記パケット網は、前記端末アドレスと通信を許されている 1 つ以上のユーザ LAN にそれぞれ割り当てられた前記識別子と端末認証に必要な情報とを対応づけた端末情報をあらかじめ記憶し、前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば前記パケット端末に対して通信許可を通知し、前記パケット端末は、前記通信許可が通知されたのであれば、1 つ以上の前記ユーザ LAN の中から通信するユーザ LAN を一つ選択し、送信すべきデータを暗号化して、該選択したユーザ LAN に割り当てられた識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には、前記受信パケットに含まれる前記送信元アドレスと前記識別子との対応が前記端末情報に登録されているかどうかを確認し、該対応が登録済みである場合には前記受信パケットを前記宛先アドレスに転送し、該対応が未登録の場合には前記受信パケットを廃棄することを特徴としている。

【 0 0 1 6 】 また、請求項 3 記載の発明は、パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザ LAN に接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、前記ユーザ LAN 毎にあらかじめ固有のユーザ LAN 名を割り当てておき、前記パケット網は、前記端末アドレスと通信を許されている 1 つ以上のユーザ LAN にそれぞれ割り当てられた前記ユーザ LAN 名と端末認証に必要な情報を対応づけた端末情報をあらかじめ記憶し、前記パケット網は前記基地局を介して通信を開始する際に、1 つ以上の前記ユーザ LAN の中から通信するユーザ LAN を一つ選択し、該選択したユーザ LAN に割り当てられた前記ユーザ LAN 名を前記パケット網へ通知し、前記パケット網は、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば、前記パケット端末から通知された前記ユーザ LAN 名に対して前記ユーザ LAN を識別するための識別子を割り当てて前記パケット端末に通知

し、前記パケット端末は、送信すべきデータを暗号化して、前記選択したユーザ LAN に割り当てられた識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には、前記受信パケットに含まれる識別子を割り当てたユーザ LAN 名と前記受信パケットに含まれる送信元アドレスとの対応が前記端末情報に登録されているかどうかを確認し、該対応が登録済みである場合には前記受信パケットを前記宛先アドレスに転送し、該対応が未登録の場合には前記受信パケットを廃棄し、前記パケット網は、その後前記パケット端末が通信を終了した時に前記ユーザ LAN 名に割り当てた前記識別子を解放するようにしたことを特徴としている。

【 0 0 1 7 】 また、請求項 4 記載の発明は、請求項 2 記載の発明において、前記パケットバックボーン網が、前記パケットを中継する複数の中継ノードを有し、これら各中継ノードが前記受信パケットを前記宛先アドレスに転送するための経路選択の機能を有するネットワークを用いたパケット転送方法であって、前記パケット網は、前記経路選択のためのルーティング情報として前記受信パケット中の前記宛先アドレスと前記識別子とを用い、ユニキャストパケットを転送する場合、前記宛先端末が前記パケット網に接続中であれば、前記宛先アドレスに応じて前記中継ノードを順次選択しながら該パケットを前記宛先端末まで転送し、前記宛先端末が前記パケット網に接続中でなければ、前記識別子に応じて前記中継ノードを順次選択しながら該パケットを前記ユーザ LAN まで転送し、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、前記識別子を用いて前記中継ノードを順次選択して該中継ノードに該パケットを順次転送してゆき、同じ識別子を用いて通信中の全ての前記パケット端末及び該識別子により指定される前記ユーザ LAN に該パケットを転送することを特徴としている。また、請求項 5 記載の発明は、請求項 2 ～ 4 の何れかの項記載の発明において、前記パケットバックボーン網と前記複数のユーザ LAN の間をゲートウェイで接続したネットワークを用いたパケット転送方法であって、前記ユーザ LAN を介して前記受信パケットを前記宛先アドレスへ転送する際、前記ゲートウェイが前記受信パケットに含まれる前記識別子に応じて前記ユーザ LAN を選択して該選択されたユーザ LAN へ前記受信パケットを転送することを特徴としている。

【 0 0 1 8 】 また、請求項 6 記載の発明は、パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン

がさらに複数の他バケット網であるユーザ LAN にゲートウェイを介して接続されているネットワークを用いたバケット通信であり、前記各バケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したバケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記バケットの転送を行うバケット転送方法であって、前記バケット網は、前記端末アドレスと端末認証に必要な情報とを対応づけた端末情報をあらかじめ記憶し、前記ゲートウェイは、前記バケット網と前記ユーザ LAN の間でバケットの転送を許可する送信元の端末アドレスをあらかじめ記憶し、前記バケット網は、前記バケット端末が前記基地局を介して通信を開始する際に、前記情報を使用して前記バケット端末の端末認証を行い、前記バケット端末が正規の端末であれば前記バケット端末に通信許可を通知し、前記バケット端末は、前記通信許可が通知されたのであれば、送信すべきデータを暗号化して前記宛先アドレスと前記送信元アドレスを付与したバケットを前記バケット網へ送信し、前記バケット網は、前記バケットを受信して該受信バケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信バケットを廃棄し、改竄されていない場合には前記受信バケットを前記ゲートウェイに転送し、前記ゲートウェイは、前記バケット網から転送されたバケットに含まれる前記送信元アドレスに対する転送が許可されている場合は該転送バケットを前記ユーザ LAN から前記宛先アドレスに転送し、該転送が許可されていない場合は該転送バケットを廃棄するようにしたことを特徴としている。

【 0 0 1 9 】 また、請求項 7 記載の発明は、請求項 6 記載の発明において、前記バケットバックボーン網が、前記バケットを中継する複数の中継ノードを有し、これら各中継ノードが前記バケットを前記宛先アドレスに転送するための経路選択機能を有するネットワークを用いたバケット転送方法であって、前記ユーザ LAN を識別する識別子を前記各ユーザ LAN にあらかじめ割り当てておき、前記バケット端末は、前記バケットを前記バケット網へ送信する際に、複数の前記ユーザ LAN の中から接続するユーザ LAN を一つ選択して、該選択したユーザ LAN の識別子を前記バケットにさらに付与して送信し、前記バケット網は、前記経路選択のためのルーティング情報として送信された前記バケットに含まれる前記宛先アドレスと前記識別子とを用い、ユニキャストバケットを転送する場合、前記宛先端末が前記バケット網に接続中であれば、前記宛先アドレスに応じて前記中継ノードを順次選択しながら該バケットを前記宛先端末まで転送し、前記宛先端末が前記バケット網に接続中でなければ、前記識別子に応じて前記中継ノードを順次選択しながら該バケットを前記ゲートウェイに転送し、ブロード

キャストバケット及びマルチキャストバケットを転送する場合は、前記識別子を用いて前記中継ノードを順次選択して該中継ノードに該バケットを順次転送してゆき、同じ識別子を用いて通信中の全ての前記バケット端末と、該識別子により指定される前記ゲートウェイとに転送することを特徴としている。

【 0 0 2 0 】 また、請求項 8 記載の発明は、請求項 4 又は 7 記載の発明において、前記暗号化及び前記復号化に際し、前記ユニキャストバケットを転送する場合は、前記各バケット端末毎に割り当てた暗号鍵を用い、前記ブロードキャストバケット又は前記マルチキャストバケットを転送する場合は、前記各識別子毎に割り当てた暗号鍵を用いることを特徴としている。また、請求項 9 記載の発明は、請求項 4 又は 7 記載の発明において、前記暗号化及び前記復号化に際し、前記ユニキャストバケットを転送する場合及び前記バケット端末が前記ブロードキャストバケット又は前記マルチキャストバケットを送信する場合は、前記各バケット端末毎に割り当てた暗号鍵を用い、前記基地局が前記ブロードキャストバケット又は前記マルチキャストバケットを送信する場合は、前記各識別子毎に割り当てた暗号鍵を用いることを特徴としている。また、請求項 1 0 記載の発明は、請求項 4 又は 7 記載の発明において、前記暗号化及び前記復号化に際し、暗号鍵として前記各識別子毎に割り当てた暗号鍵を用いることを特徴としている。

【 0 0 2 1 】 また、請求項 1 1 記載の発明は、他バケット網であるユーザ LAN が複数接続されたバケットバックボーン網に接続され、かつ、配下に複数のバケット端末を収容する基地局であって、前記各バケット端末に付与された固有の端末アドレスと、前記バケット端末が通信を許されている 1 つ以上のユーザ LAN にそれぞれ割り当てられた識別子と、端末認証に必要な情報を対応づけて記憶する端末情報記憶手段と、前記バケット端末からの通信開始要求に応じて前記情報を使用した端末認証を行い、前記バケット端末に対して認証結果を通知する端末認証手段と、前記バケットバックボーン網と前記バケット端末の間で授受されるバケット中のデータ部を前記情報を用いて暗号化して送信するバケット暗号化手段と、宛先端末の前記端末アドレスである宛先アドレスと前記バケット端末の端末アドレスである送信元アドレスと前記ユーザ LAN に割り当てられた識別子が暗号化データに付与されたバケットを前記バケット端末から受信して該暗号化データを復号するバケット復号化手段と、前記復号されたデータから改竄を検出して該バケットを廃棄するバケット改竄検出手段と、前記バケットに含まれている前記送信元アドレス及び前記識別子の組が、前記端末情報記憶手段に記憶されている前記端末アドレス及び前記識別子の組の中に登録されているかどうかを確認する比較手段と、前記比較手段による確認結果に基づいて、前記登録があることを条件に前記宛先アドレスに

前記パケットを転送し、前記登録が無いことを条件に前記パケットを廃棄するフィルタリング手段とを具備することを特徴としている。

【 0 0 2 2 】 また、請求項 1 2 記載の発明は、他パケット網であるユーザ LAN が複数接続されたパケットバックボーン網に接続され、かつ、配下に複数のパケット端末を收容する基地局であって、前記各パケット端末に付与された固有の端末アドレスと、前記パケット端末が通信を許されている 1 つ以上のユーザ LAN にそれぞれ割り当てられたユーザ LAN 名と、端末認証に必要な情報を対比づけて記憶する端末情報記憶手段と、前記パケット端末からの通信開始要求に応じて前記情報を使用した端末認証を行って、認証結果を前記パケット端末に通知するとともに、正規のパケット端末に対しては、前記通信開始要求に伴って前記パケット端末から通知されるユーザ LAN 名に前記ユーザ LAN を識別するための識別子を割り当てて通知し、前記パケット端末が通信を終了したことを条件として前記ユーザ LAN 名に割り当てた前記識別子を解放する端末認証手段と、前記パケットバックボーン網と前記パケット端末の間で授受されるパケット中のデータ部を前記情報を用いて暗号化して送信するパケット暗号化手段と、宛先端末の前記端末アドレスである宛先アドレスと前記パケット端末の端末アドレスである送信元アドレスと前記識別子が暗号化データに付与されたパケットを前記パケット端末から受信して該暗号化データを復号するパケット復号化手段と、前記復号されたデータから改竄を検出して該パケットを廃棄するパケット改竄検出手段と、前記受信したパケットに含まれる識別子を割り当てたユーザ LAN 名と前記受信したパケットに含まれる送信元アドレスの組が、前記端末情報記憶手段に記憶されている前記ユーザ LAN 名及び前記端末アドレスの組の中に登録されているかどうかを確認する比較手段と、前記比較手段による確認結果に基づいて、前記登録があることを条件に前記宛先アドレスに前記パケットを転送し、前記登録が無いことを条件に前記パケットを廃棄するフィルタリング手段とを具備することを特徴としている。

【 0 0 2 3 】 また、請求項 1 3 記載の発明は、請求項 1 1 記載の発明において、前記パケット暗号化手段は、送信するパケットがユニキャストパケットであれば、各パケット端末毎に割り当てた暗号鍵を用いて暗号化し、前記送信するパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて暗号化し、前記パケット復号化手段は、受信したパケットがユニキャストパケットであれば、前記各パケット端末毎に割り当てた暗号鍵を用いて復号化し、前記受信したパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて復号化することを特徴としている。また、請求項 1 4 記載の発明は、請求項

1 1 記載の発明において、前記パケット暗号化手段は、送信するパケットがユニキャストパケットであれば、各パケット端末毎に割り当てた暗号鍵を用いて暗号化し、前記送信するパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて暗号化し、前記パケット復号化手段は、前記各パケット端末毎に割り当てた暗号鍵を用いて復号化することを特徴としている。また、請求項 1 5 記載の発明は、請求項 1 1 記載の発明において、前記パケット暗号化手段は、前記各識別子毎に割り当てた暗号鍵を用いて送信するパケットのデータ部を暗号化し、前記パケット復号化手段は、前記各識別子毎に割り当てた暗号鍵を用いて受信したパケットのデータ部を復号することを特徴としている。

【 0 0 2 4 】

【発明の実施の形態】 以下、本発明の種々の実施形態について、図面を参照して説明する。なお、本発明は無線パケット網、有線パケット網の何れに対しても適用することができるが、以下では無線パケット網を中心にして説明を行い、最後に有線パケット網へ適用する場合の実施形態について説明する。

【 0 0 2 5 】 【第 1 実施形態】 この第 1 実施形態は、請求項 1, 2, 5 記載のパケット転送方法および請求項 1 1 記載の基地局を適用した場合に相当している。

【 0 0 2 6 】 図 1 は、本実施形態におけるパケット網のネットワーク構成を概略的に示している。同図において、複数の無線基地局 1 - 6 と、これら無線基地局 1 - 6 を接続する無線パケットバックボーン網 1 - 5 とで構成されるものを無線パケット網とする。各無線基地局 1 - 6 は配下に複数の無線パケット端末 1 - 7 を收容している。ユーザ LAN 1 - 4 は他パケット網であって、無線パケットバックボーン網 1 - 5 はゲートウェイ 1 - 1 ~ 1 - 3 を介して複数のユーザ LAN 1 - 4 に接続している。ゲートウェイ 1 - 3 は後述する VLAN-ID に応じて何れかのユーザ LAN 1 - 4 を選択し、パケットから VLAN-ID を削除したのち、選択したユーザ LAN へパケットを転送する。無線パケットバックボーン網 1 - 5 とユーザ LAN 1 - 4 との間の中継路 1 - 1 0 としては、ATM (Asynchronous Transfer Mode; 非同期転送モード) 網のバーチャルチャネルコネクション (VCC), インターネット上のバーチャルプライベートネットワーク (VPN) 等の各種のものが選択可能である。また、無線パケットバックボーン網 1 - 5 は端末認証サーバ 1 - 8 に接続されている。この端末認証サーバ 1 - 8 は端末情報テーブルを記憶しており、無線パケット端末 1 - 7 が通信を開始する時に無線基地局 1 - 6 へ端末情報を与える。

【 0 0 2 7 】 本実施形態において、端末情報テーブルは少なくとも端末アドレスと、後述する VLAN-ID と、端末認証に必要な情報として各端末固有の暗号鍵と

を組にして持っている。端末アドレスとしてはイーサネットにおける MAC (Media Access Control) アドレスを用いる。なお、無線パケット網はあらかじめ各無線パケット端末に暗号鍵を通知しておく。

【0028】ここで、図2は本実施形態による無線基地局1-6の構成を示している。無線基地局1-6に設けられている各手段が有する機能については、これ以後の説明の中で順次説明してゆく。なお、同図において、実線は無線パケットバックボーン網1-5又は無線パケット端末1-7と無線基地局1-6との間で送受信されるパケット信号を意味しており、破線は無線基地局1-6内の各部間の制御信号を意味している。

【0029】図3は、本実施形態における無線パケット端末1-7の認証手順を示している。同図に示すように、無線パケット端末1-7は通信を開始する時に通信開始要求信号を無線基地局1-6へ送信する(2-1)。無線基地局1-6では、端末認証手段10が通信開始要求信号を受信して、端末認証サーバ1-8に端末情報要求を行う(2-2)。この端末情報要求に対して端末認証サーバ1-8が端末情報通知を無線基地局1-6に行うと、端末認証手段10はこの端末情報通知を受けて(2-3)、通知された端末情報を端末情報記憶手段11に記憶させる。次に、端末認証手段10は端末認証用の乱数を生成したのち、端末情報に含まれている暗号鍵を用いて暗号化し、暗号化された乱数を認証要求信号として無線パケット端末1-7に送信する(2-4)。無線パケット端末1-7は無線パケット網から通知されている暗号鍵で送信された乱数を復号化し、これを認証応答信号として無線基地局1-6に送り返す(2-5)。無線基地局1-6では、端末認証手段10が認証要求信号として送信した乱数と送り返された乱数を比較する。両者が一致する場合、端末認証手段10は無線パケット端末1-7を正規端末と判断し、認証受付信号を用いて無線パケット端末1-7に通信許可を通知する(2-6)。これ以後は、パケット暗号化手段12が端末認証手段10から取得した暗号鍵を用いて、データパケット中のヘッダ部を除いたデータ部だけを暗号化して転送を行う。一方、上記2つの乱数が一致しない場合、端末認証手段10は無線パケット端末1-7を不正端末と判断し、認証受付信号を用いて無線パケット端末1-7に通信拒否を通知する(2-6)。

【0030】図4は、本実施形態におけるデータパケットの改竄検出手順を示している。無線パケット端末1-7は、生じたデータに対する誤り検出符号を計算して当該データに付与してから暗号化し、さらにヘッダ情報を付与したデータパケットを無線基地局1-6に送信する(3-1)。無線基地局1-6では、パケット復号化手段13がデータパケット中の暗号化されたデータ部を復号してパケット改竄検出手段14に送出する。パケット改竄検出手段14は復号されたデータの誤り検出符号

を計算し、この計算された誤り検出符号と復号によってパケットから得た誤り検出符号とを比較して、両者が一致する場合は改竄無しと判断し、両者が一致しない場合は改竄ありと判断する。

【0031】表1は、本実施形態における端末情報テーブルを示している。端末情報テーブルは、端末アドレスと、VLAN-IDと、端末認証に必要な情報としての暗号鍵とからなる端末情報で構成されている。なお、この端末情報は端末認証手段10が端末情報記憶手段11へ記憶させる(図2を参照)。

【0032】

【表1】

第1の実施形態における端末情報テーブル

端末アドレス	VLAN-ID	暗号鍵
アドレス#1	VLAN-ID#A	暗号鍵#a
アドレス#2	VLAN-ID#A	暗号鍵#b
アドレス#3	VLAN-ID#B	暗号鍵#c

【0033】このVLAN-IDはユーザLAN1-4を識別するための識別子として定義され、各ユーザLANに固有の値があらかじめ割り当てられている。無線パケット端末1-7は、自分の所属するユーザLAN1-4のVLAN-IDをそれぞれ端末認証サーバ1-8にあらかじめ登録している。

【0034】図5は、本実施形態における無線パケット網が使用するパケットの信号フォーマットを示している。同図に示すように、パケットはヘッダ情報として宛先アドレス4-1、送信元アドレス4-2及びVLAN-ID4-3を持っており、ユーザデータ4-4の部分

は暗号化されている。【0035】以下に詳述するように、無線基地局1-6は、無線パケット端末1-7から受信したパケットの内、VLAN-ID4-3が当該無線パケット端末の所属するユーザLAN1-4のVLAN-IDに一致するパケットのみを転送し、これらVLAN-IDが一致しないパケットは廃棄する。

【0036】図6は、本実施形態におけるパケット転送手順を示している。無線基地局1-6は通信開始時に図3に示した認証を行い、無線パケット端末1-7が正規端末であると判断された場合には通信を開始させる。次に、無線基地局1-6は図4に示した改竄検出手順を行い、無線パケット端末1-7から受信したデータパケット(5-1)の改竄を検出した場合はこのデータパケットを廃棄する。一方で改竄が検出されない場合、無線基地局1-6では、端末アドレス/VLAN-ID比較手段15が端末情報記憶手段11に記憶してある端末情報を参照し、VLAN-IDと送信元アドレス4-2との対応を確認してその結果をフィルタリング手段16に送出する。すなわち、端末アドレス/VLAN-ID比較手段15は、表1に示す端末情報テーブルを検索して、

端末アドレス、VLAN-IDがそれぞれデータパケット中の送信元アドレス4-2、VLAN-ID4-3に等しいものが存在すれば、上記対応が端末情報に一致しているものと判断する。フィルタリング手段16は送られた確認結果に基づき、上記対応が端末情報に一致していれば宛先アドレス4-1で指定された宛先端末にデータパケットを転送する(5-2)。この時、宛先端末がユーザLAN1-4と接続していれば、データパケットはゲートウェイ1-3からゲートウェイ1-1又はゲートウェイ1-2を介してユーザLAN1-4に転送される。また、宛先端末が無線パケット網と接続している場合、データパケットはゲートウェイを介することなく宛先端末に転送される。一方、VLAN-IDと送信元アドレス4-2との対応が端末情報に一致していない場合、フィルタリング手段16はデータパケットを廃棄する。

【0037】ここで、ユーザLAN1-4から無線パケット端末1-7へパケットを転送する場合の手順について簡単に説明しておく。ユーザLAN1-4が自身に接続しているゲートウェイ1-1又はゲートウェイ1-2にパケットを送信すると、これらゲートウェイは送信されたパケットを中継路1-10からゲートウェイ1-3に転送する。ゲートウェイ1-3は、パケットが送られてきた中継路1-10に応じて送信元のユーザLAN1-4に割り当てられているVLAN-IDをパケットに付与したのちに無線パケットバックボーン網1-5に転送する。無線基地局1-6は転送されてきたパケットを受信し、当該パケットのデータ部を暗号化して宛先アドレスが示す無線パケット端末1-7へ送信し、無線パケット端末1-7は暗号化されたパケットを受信して復号する。

【0038】以上のように、本実施形態によれば、通信開始時に端末認証することによって無線パケット端末を特定可能であり、未知の端末や端末アドレスを偽造した

第2の実施形態における端末情報テーブル

端末アドレス	VLAN-ID	VLAN-ID	暗号鍵
アドレス#1	VLAN-ID#A	VLAN-ID#B	暗号鍵#a
アドレス#2	VLAN-ID#A	VLAN-ID#B	暗号鍵#b
アドレス#3	VLAN-ID#B	—	暗号鍵#c

【0045】以下に詳述するように、無線基地局1-6は、無線パケット端末1-7から受信したパケットの内、当該無線パケット端末が接続を許可されているユーザLANのVLAN-IDの何れかとVLAN-ID4-3が一致するパケットのみを転送し、何れのVLAN-IDにも一致しないパケットは廃棄する。

【0046】図7は、本実施形態におけるパケット転送手順を示している。無線基地局1-6では端末認証手段10が無線パケット端末1-7に対する認証を行い、当該無線パケット端末が正規の端末であれば暗号通信を開

端末からの不正アクセスを防止することができる。また、端末固有の暗号鍵により暗号化してパケットを転送することにより、不正な端末が認証された正規の端末になりすますことを防止可能であり、なりすまし端末による不正アクセスを防止することができる。さらに、暗号の復号時に改竄を検出してパケットを廃棄することにより、改竄されたパケットの転送を防止可能であり、改竄データによる通信の妨害と無線パケット網のトラヒック増加を防止する効果が得られる。しかも、VLAN-IDと送信元アドレスの対応を確認することにより、認証後の端末が自分の属していないユーザLANにアクセスすることを防止可能であり、他ユーザLANに所属している端末からの不正アクセスを防止することができる。

【0039】〔第2実施形態〕この第2実施形態は、請求項1、2、5記載のパケット転送方法および請求項11記載の基地局を適用した場合に相当している。

【0040】本実施形態において、パケット網のネットワーク構成、無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、それぞれ図1～図5に示した第1実施形態の場合と等しい。

【0041】第1実施形態と同様に、VLAN-IDは各ユーザLAN1-4に固有の値があらかじめ割り当てられている。

【0042】各無線パケット端末1-7は、接続を許可されている複数のユーザLAN1-4のVLAN-IDを端末認証サーバ1-8にあらかじめ登録している。

【0043】表2は、本実施形態における端末情報テーブルを示している。例えば、端末アドレスとしてアドレス#1を持つ無線パケット端末は、VLAN-IDとしてVLAN-ID#A又はVLAN-ID#Bを持つユーザLAN1-4に接続が許可されている。

【0044】

〔表2〕

始する。次に、無線基地局1-6ではパケット復号化手段13が無線パケット端末1-7からのデータパケットを復号(6-1)し、パケット改竄検出手段14は受信データパケットの改竄を調べ、改竄が検出された場合はパケットを廃棄する。なお、これまでの手順は第1実施形態と同様である。一方、改竄が検出されない場合、無線基地局1-6では、端末アドレス/VLAN-ID比較手段15が端末情報記憶手段11に記憶してある端末情報を参照し、VLAN-ID4-3と送信元アドレス4-2との対応が端末情報に登録済みであるかどうか確

認してその結果をフィルタリング手段 16 に送出する。
すなわち、端末アドレス/VLAN-ID 比較手段 15
は、端末情報テーブル中の端末アドレスが送信元アド
レス 4-2 に一致し、かつ、当該端末アドレスに対応して
登録されている複数の VLAN-ID の中に VLAN-ID
4-3 と一致するものが存在していれば、上記対応
が端末情報に登録済みであるものと判断する。そして、
フィルタリング手段 16 は送られた確認結果に基づい
て、上記対応が端末情報に登録済みであれば宛先アド
レス 4-1 で指定された宛先端末にデータパケットを転送
する(6-2)。この時、宛先端末がユーザ LAN 1-
4 と接続しているならば、データパケットはゲートウェ
イ 1-3 からゲートウェイ 1-1 又はゲートウェイ 1-
2 を介してユーザ LAN 1-4 に転送される。また、宛
先端末が無線パケット網と接続している場合、データパ
ケットはゲートウェイを介することなく宛先端末に転送
される。一方、VLAN-ID と送信元アドレスとの対
応が端末情報に未登録の場合、フィルタリング手段 16
はデータパケットを廃棄する。

【0047】以上のように、本実施形態によれば、第 1
実施形態から得られる効果のほかにさらに以下の効果が
得られる。すなわち、VLAN-ID と送信元アドレス
の対応を確認することにより、認証後の端末が接続の許
可されていないデータ網にアクセスすることを防止可能
であり、接続を許可されている端末から他データ網への
不正アクセスを防止することができる。また、1 無線パ
ケット端末あたり複数の VLAN-ID を登録すること
により、1 つの無線パケット端末で複数のデータ網にア
クセスすることが可能であり、ユーザへのサービス性が
向上する。

【0048】〔第 3 実施形態〕この第 3 実施形態は、請
求項 1, 2, 4, 5, 8 記載のパケット転送方法および
請求項 11, 13 記載の基地局を適用した場合に相当し
ている。

【0049】図 8 は、本実施形態におけるパケット網の
ネットワーク構成を概略的に示している。第 1 実施形態
と同様に、無線パケット網は、複数の無線基地局 7-6
と、これら複数の無線基地局 7-6 を接続する無線パケ
ットバックボーン網 7-5 とで構成されている。各無線
基地局 7-6 はその配下に複数の無線パケット端末 7-7
を収容している。無線パケットバックボーン網 7-5
は、ゲートウェイ 7-1~7-3 を介して、複数のユー
ザ LAN 7-4 (他パケット網) に接続されている。こ
こで、ゲートウェイ 7-3 は VLAN-ID 4-3 に応
じて何れかのユーザ LAN 7-4 を選択し、パケットか
ら VLAN-ID を削除したのち、選択したユーザ LAN
へパケットを転送する。さらに、本実施形態における
無線パケットバックボーン網 7-5 はパケットを中継す
る複数の中継ノード 7-9 を有している。各中継ノード
7-9 は、パケット中の宛先アドレス 4-1 及び VLA

N-ID 4-3 を用いたルーティング情報を有しており、
このルーティング情報に従って最適な経路を選択してパケ
ットを転送する。例えば、中継ノード 7-9 は、パケッ
トを受信した時に、受信パケット中の送信元アドレス 4
-2 が示す宛先アドレスと当該パケットを受信したポー
ト、および、受信パケット中の VLAN-ID 4-3 と
当該パケットを受信したポートを対応づけて記憶する。
次に、中継ノード 7-9 は、受信パケットがユニキャスト
パケットならば、宛先アドレス 4-1 が示す宛先アド
レスに対応するポートへ受信パケットを送信する。これ
に対し、受信パケットがブロードキャストパケット又は
マルチキャストパケットならば、中継ノード 7-9 は V
LAN-ID 4-3 に対応する全てのポートへ受信パケ
ットを送信する。なお、ここで言う“ポート”は、中継
ノード 7-9 が自身に隣接する中継ノード又は無線基地
局との間の通信路を接続するためのインタフェースであ
る。また、中継路 7-10 としては、図 1 に示した中継
路 1-10 と同様に各種のものが選択可能である。ま
た、無線パケットバックボーン網 7-5 は中継ノード 7
-9 を介して端末認証サーバ 7-8 に接続されている。
端末認証サーバ 7-8 は図 1 に示した端末認証サーバ 1
-8 と同じく表 2 に示した端末情報テーブルを記憶して
おり、無線パケット端末 7-7 が通信を開始する際に無
線基地局 7-6 に対して端末情報を与える。

【0050】本実施形態において、この端末情報テー
ブルに登録された暗号鍵は端末認証及びユニキャストパケ
ットの暗号化に用いられ、以下ではこの暗号鍵を「端末
鍵」という。なお、無線パケット網は各無線パケット端
末 7-7 に端末鍵をあらかじめ通知しておく。

【0051】以上に加えて、端末認証サーバ 7-8 は表
3 に示す VLAN 情報テーブルに VLAN 情報を持って
いる。

【0052】

〔表 3〕

第 3 の実施形態における VLAN 情報テーブル

VLAN-ID	VLAN 鍵
VLAN-ID#A	VLAN 鍵#a
VLAN-ID#B	VLAN 鍵#b

【0053】この VLAN 情報テーブルは、VLAN-ID
と、同じ VLAN-ID を持つ全ての端末で共通に
使用する暗号鍵(以下、「VLAN 鍵」という)との対
応を記録している。この VLAN 鍵はブロードキャスト
パケット及びマルチキャストパケットの暗号化に使用さ
れる。なお、無線パケット網は各無線パケット端末 7-
7 に対して VLAN 鍵をあらかじめ通知しておく。

【0054】第 1 実施形態と同様に、VLAN-ID は
各ユーザ LAN 7-4 に固有の値があらかじめ割り当て
られている。

【 0 0 5 5 】 無線パケット端末 7 - 7 は自分の所属するユーザ LAN 7 - 4 の VLAN - ID をそれぞれ端末認証サーバ 7 - 8 の端末情報テーブルにあらかじめ登録している。

【 0 0 5 6 】 以下に詳述するように、無線基地局 7 - 6 は、無線パケット端末 7 - 7 から受信したパケットの内、当該無線パケット端末が接続を許可されているユーザ LAN 7 - 4 の VLAN - ID の何れかと VLAN - ID 4 - 3 が一致するパケットのみを転送し、何れの VLAN - ID にも一致しないパケットは廃棄する。

【 0 0 5 7 】 本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図 2 ～ 図 5 に示した第 1 実施形態の場合とそれぞれ等しい。

【 0 0 5 8 】 図 9 は、本実施形態におけるパケット転送手順を示している。第 1 実施形態と同様に、無線基地局 7 - 6 では、端末認証手段 1 0 が通信開始時に無線パケット端末 7 - 7 に対する認証を行い、当該無線パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して、端末認証手段 1 0 は端末認証サーバ 7 - 8 から端末情報と共に VLAN 情報を得て端末情報記憶手段 1 1 に記憶させる。一方、無線パケット端末 7 - 7 は、ユニキャストパケットを送信する時には端末鍵を選択して暗号化を行い、暗号化されたデータパケットを無線基地局 7 - 6 に送信する (8 - 1)。一方、無線パケット端末 7 - 7 は、ブロードキャストパケット又はマルチキャストパケットを送信する時には VLAN 鍵を選択して暗号化を行い、暗号化されたデータパケットを無線基地局 7 - 6 に送信する (8 - 1)。これらに対応して、無線基地局 7 - 6 のパケット復号化手段 1 3 は、ユニキャストパケットを受信した時には端末鍵を選択してデータパケットを復号し、また、ブロードキャストパケット又はマルチキャストパケットを受信した時には VLAN 鍵を選択してデータパケットを復号する。パケット改竄検出手段 1 4 は、図 4 に示した改竄検出手順に従って復号されたデータパケットの改竄の有無を調べ、改竄が検出された場合にはデータパケットを廃棄する。一方、データパケットの改竄が検出されない場合、端末アドレス / VLAN - ID 比較手段 1 5 は、第 2 実施形態と同様にして VLAN - ID 4 - 3 と送信元アドレス 4 - 2 の対応を確認し、これらの対応が端末情報に登録済みであれば宛先アドレスで指定された宛先端末にデータパケットを転送する (8 - 2)。この時、本実施形態では、宛先端末がユーザ LAN 7 - 4 と接続している場合、各中継ノード 7 - 9 はデータパケット中の宛先アドレス 4 - 1 に応じて次の送信ポートを選択してゲートウェイ 7 - 3 へデータパケットを転送する。ゲートウェイ 7 - 3 は VLAN - ID 4 - 3 に応じてゲートウェイ 7 - 1 又はゲートウェイ 7 - 2 の何れかを選択してデータパケットをユーザ LAN 7 - 4 に転送する。また、宛先

端末が無線パケット網と接続している場合、各中継ノード 7 - 9 は宛先アドレス 4 - 1 に応じて次の送信ポートを選択してデータパケットを宛先端末へ転送する。したがってこの場合はゲートウェイを介することなくデータパケットが転送される。一方、VLAN - ID と送信元アドレスとの対応が端末情報に登録されていない場合、フィルタリング手段 1 6 はデータパケットを廃棄する。

【 0 0 5 9 】 図 1 0 は、本実施形態におけるブロードキャストパケットの転送手順を示している。送信元端末ではデータが生起するとブロードキャストパケットを無線基地局 7 - 6 に送信する (9 - 1)。無線基地局 7 - 6 では、パケット暗号化手段 1 2 が端末認証手段 1 0 から取得した暗号鍵のうち VLAN 鍵を選択 (9 - 2) してブロードキャストパケットを暗号化 (9 - 3) し、全てのパケット端末 (同図では無線パケット端末 # 1, # 2) へブロードキャストパケットを送信する (9 - 4)。各無線パケット端末 # 1, # 2 では、暗号鍵として VLAN 鍵を選択 (9 - 5) し、暗号化されたブロードキャストパケットを復号化する (9 - 6)。このように本実施形態では、暗号化に VLAN 鍵を用いているため、同じ VLAN - ID を有するパケット端末がブロードキャストパケット及びマルチキャストパケットを復号化することが可能である。

【 0 0 6 0 】 図 1 1 は、ブロードキャストパケットがネットワーク内を転送されてゆく様子を示している。同図に示すように、ユーザ LAN # A に属する無線パケット端末 7 - 7 a (送信端末) がブロードキャストパケットを無線基地局 7 - 6 a に送信すると、このパケットは無線パケットバックボーン網 7 - 5 に送出される。無線パケットバックボーン網 7 - 5 は、VLAN - ID 4 - 3 に応じて中継ノード 7 - 9 a からゲートウェイ 7 - 3 及び中継ノード 7 - 9 b にブロードキャストパケットを転送する。ここで、ゲートウェイ 7 - 3 は VLAN - ID 4 - 3 を見て、ユーザ LAN # A に接続されたゲートウェイ 7 - 1 へブロードキャストパケットを転送する。一方、中継ノード 7 - 9 b はブロードキャストパケットをさらに中継ノード 7 - 9 c と転送し、中継ノード 7 - 9 c は、ユーザ LAN # A に属する無線パケット端末 7 - 7 c が接続された無線基地局 7 - 6 c にブロードキャストパケットを転送する。

【 0 0 6 1 】 このように、VLAN - ID を用いたルーティング情報によって経路が選択されてブロードキャストパケットが転送される。また、無線基地局 7 - 6 b にはユーザ LAN # B に属する無線パケット端末 7 - 7 b のみが接続されており、VLAN - ID 4 - 3 と同じ VLAN - ID を有する無線パケット端末を配下に持っていない。したがって、中継ノード 7 - 9 b は無線基地局 7 - 6 b に対してブロードキャストパケットを転送しない。

【 0 0 6 2 】 なお、上述した説明では第 2 実施形態を基

にしたパケット転送手順について説明したが、第 1 実施形態を基にしても良い。そうした場合、端末情報テーブルとしては表 2 の代わりに表 1 を使用することになるほか、VLAN-ID と送信元アドレスの対応が端末情報に登録済みであるか確認する（図 9 における 8-3）代わりに、この対応が端末情報に一致するかどうか確認することになる（図 6 における 5-3）。

【0063】以上のように、本実施形態によれば第 1 ～ 第 2 実施形態に加えて以下の効果が得られる。すなわち、本実施形態では、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【0064】また、ブロードキャストパケット又はマルチキャストパケットを転送する場合は、VLAN-ID に応じて次の中継ノードを選択して転送するため、同じ VLAN-ID を用いて通信している全ての無線パケット端末に対してゲートウェイからユニキャスト転送する必要がない。したがって、最適な経路選択でパケットを転送することが可能であり、転送遅延時間、トラヒック、ゲートウェイの処理負荷の増加をそれぞれ防止することができる。

【0065】また、VLAN-ID が同じであれば共通の暗号鍵を用いてブロードキャストパケット又はマルチキャストパケットを暗号化しているため、無線基地局は、同一の VLAN-ID を持つ配下の全無線パケット端末に対して、1 回の送信でブロードキャストパケット又はマルチキャストパケットを転送することが可能となる。したがって、各無線パケット端末の暗号鍵を用いて暗号化したパケットを複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷を抑制することができる。なお、VLAN 鍵は端末固有の暗号鍵ではないが、異なる VLAN-ID を持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【0066】〔第 4 実施形態〕この第 4 実施形態は、請求項 1, 2, 4, 5, 9 記載のパケット転送方法および請求項 11, 14 記載の基地局を適用した場合に相当している。

【0067】本実施形態におけるパケット網のネットワーク構成は図 8 に示した第 3 実施形態の構成に等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図 2 ～ 図 5 に示した第 1 実施形態の場合とそれぞれ等しい。

【0068】第 3 実施形態と同様に、VLAN-ID は各ユーザ LAN 7-4 に固有の値があらかじめ割り当てられている。

【0069】無線パケット端末 7-7 は、自分の所属するユーザ LAN 7-4 の VLAN-ID をあらかじめ端末認証サーバ 7-8 の端末情報テーブルに登録している。

【0070】第 3 実施形態と同様に、無線基地局 7-6 は、無線パケット端末 7-7 から受信したパケットの内、当該無線パケット端末が接続を許可されているユーザ LAN 7-4 の VLAN-ID の何れかと VLAN-ID 4-3 が一致するパケットのみを転送し、何れの VLAN-ID にも一致しないパケットは廃棄する。

【0071】また、端末認証サーバ 7-8 は表 3 に示した第 3 実施形態と同じ VLAN 情報テーブルを持っており、VLAN 鍵はブロードキャストパケット及びマルチキャストパケットの暗号化に使用される、無線パケット網が各無線パケット端末 7-7 に VLAN 鍵をあらかじめ通知しておくことも第 3 実施形態と同じである。

【0072】本実施形態における端末情報テーブルは表 2 に示した第 2 実施形態の端末情報テーブルと等しい。この端末情報テーブルに登録された暗号鍵（端末鍵）

は、端末認証時、ユニキャストパケットの暗号化時、ならびに、無線パケット端末によるブロードキャスト及びマルチキャストパケットの暗号化時にそれぞれ用いられる。なお、無線パケット網は各無線パケット端末 7-7 に端末鍵をあらかじめ通知しておく。

【0073】図 12 は、本実施形態におけるパケット転送手順を示している。無線基地局 7-6 では、第 3 実施形態と同様にして、端末認証手段 10 が通信開始時において無線パケット端末 7-7 に対する認証を行い、当該パケット端末が正規の端末であれば暗号通信を開始する。

なお、この認証に際して端末認証手段 10 が端末認証サーバ 7-8 から端末情報と共に VLAN 情報を得るのも第 3 実施形態と同じである。次に、第 3 実施形態とは異なっており、無線パケット端末 7-7 はユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なく端末鍵を用いてデータパケットを暗号化して無線基地局 7-6 に送信する（11-1）。無線基地局 7-6 では、パケット復号化手段 13 がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなく端末鍵を用いてデータパケットを復号化する。そしてこれ以後の手順は第 3 実施形態と同じである。無線基地局 7-6 は、受信したデータパケットが改竄されていればデータパケットを廃棄し、改竄されていなければ VLAN-ID と送信元アドレスとの対応が端末情報に登録済みであれば宛先アドレス 4-1 で指定される宛先端末にデータパケットを転送する（11-2）。このとき、データパケットは第 3 実施形態と同様に転送されてゆく。一方、VLAN-ID と送信元アドレスとの対応が端末情報に登録されていない場合、フィルタリング手段 16 はデータパケットを廃棄する。

【 0 0 7 4 】本実施形態では、無線基地局 7 - 6 が送信するブロードキャストパケット及びマルチキャストパケットの暗号化の際には第 3 実施形態と同様に V L A N 鍵を用いるため、同じ V L A N - I D を有するパケット端末はブロードキャストパケット及びマルチキャストパケットの復号が可能である。一方、無線パケット端末 7 - 7 が送信するブロードキャストパケット及びマルチキャストパケットの暗号化には端末鍵を用いているため、無線基地局 7 - 6 は第 3 実施形態のように 2 種類の暗号鍵（端末鍵、V L A N 鍵）を切り替えて暗号を復号化する必要がない。

【 0 0 7 5 】また、本実施形態においてブロードキャストパケットをパケット網で転送する様子は、図 1 0 ~ 図 1 1 に示す第 3 実施形態の場合に等しい。すなわち、無線基地局 7 - 6 がブロードキャスト又はマルチキャストパケットを送信する場合には、V L A N 鍵を用いてパケットの暗号化が行われることになる。

【 0 0 7 6 】なお、上述した説明では第 2 実施形態を基にしたパケット転送手順について説明したが、第 1 実施形態を基にしても良い。その場合には、第 3 実施形態で説明したように、表 1 に示す端末情報テーブルを使用するとともに、V L A N - I D と送信元アドレスの対応が端末情報に一致するかどうか確認することになる。

【 0 0 7 7 】以上のように、本実施形態によれば、第 3 実施形態と同様に、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【 0 0 7 8 】これに加えて本実施形態では、無線基地局がブロードキャストパケット又はマルチキャストパケットを転送する際には、V L A N - I D に共通する暗号鍵を用いて暗号化している。このため、無線基地局は同じ V L A N - I D を持つ配下の全無線パケット端末に対して 1 回の送信でパケット転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制することができる。

【 0 0 7 9 】また、無線パケット端末がブロードキャストパケット又はマルチキャストパケットを転送する際、ユニキャストパケット用の暗号鍵を用いて暗号化している。したがって、無線基地局は無線パケット端末からパケットを受信した時に暗号鍵を切り替えることなく復号することが可能となり、ブロードキャストパケット及びマルチキャストパケット用の暗号鍵を用いて暗号化して送信する場合に比べて、無線基地局にかかる負荷を抑制することができる。

【 0 0 8 0 】〔第 5 実施形態〕この第 5 実施形態は、請求項 1、2、4、5、1 0 記載のパケット転送方法および請求項 1 1、1 5 記載の基地局を適用した場合に相当

している。

【 0 0 8 1 】本実施形態におけるパケット網のネットワーク構成は、図 8 に示す第 3 実施形態の構成に等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図 2 ~ 図 5 に示した第 1 実施形態の場合とそれぞれ等しい。

【 0 0 8 2 】第 3 実施形態と同様に、V L A N - I D は各ユーザ L A N 7 - 4 に固有の値があらかじめ割り当てられている。

【 0 0 8 3 】端末認証サーバ 7 - 8 は第 3 実施形態と同様に端末情報テーブル及び V L A N 情報テーブルを有している。

【 0 0 8 4 】第 3 実施形態と同様に、無線基地局 7 - 6 は、無線パケット端末 7 - 7 から受信したパケットの内、当該無線パケット端末が接続を許可されているユーザ L A N 7 - 4 の V L A N - I D の何れかと V L A N - I D 4 - 3 が一致するパケットのみを転送し、何れの V L A N - I D にも一致しないパケットは廃棄する。

【 0 0 8 5 】本実施形態では、V L A N 鍵はパケットを暗号化するときを使用される。なお、無線パケット網は各無線パケット端末 7 - 7 に V L A N 鍵をあらかじめ通知しておく。

【 0 0 8 6 】本実施形態における端末情報テーブルは、表 2 に示した第 2 実施形態の端末情報テーブルと等しい。ここで、本実施形態ではこの端末情報テーブルに登録する暗号鍵として、各パケット端末が所属するユーザ L A N 7 - 4 の V L A N 鍵を用いる。

【 0 0 8 7 】図 1 3 は、本実施形態におけるパケット転送手順を示している。第 3 実施形態と同様に、無線基地局 7 - 6 では端末認証手段 1 0 が通信開始時に無線パケット端末 7 - 7 に対する認証を行い、当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証サーバ 7 - 8 から端末情報と共に V L A N 情報を得るのも第 3 実施形態と同じである。次に、第 3 実施形態及び第 4 実施形態とは異なって、無線パケット端末 7 - 7 はユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なく V L A N 鍵を用いてデータパケットを暗号化して無線基地局 7 - 6 に送信する（1 2 - 1）。無線基地局 7 - 6 では、パケット復号化手段 1 3 がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなく V L A N 鍵を用いてデータパケットを復号化する。そしてこれ以後の手順は第 3 実施形態と同じである。無線基地局 7 - 6 は、受信したデータパケットが改竄されていればパケットを廃棄し、改竄されていなければ V L A N - I D と送信元アドレスとの対応が端末情報に登録済みであれば宛先アドレス 4 - 1 で指定される宛先端末にデータパケットを転送する（1 2 - 2）。このとき、データパケットは第 3 実施形態と同様

に転送されてゆく。一方、VLAN-IDと送信元アドレスとの対応が端末情報に登録されていない場合、フィルタリング手段16はデータパケットを廃棄する。

【0088】本実施形態では、第3実施形態と違って暗号化にVLAN鍵のみを用いるようにして端末鍵を用いていないため、同じVLAN-IDを有する無線パケット端末が、ブロードキャストパケット及びマルチキャストパケットに施された暗号を復号化することが可能である。また、無線基地局及び無線パケット端末は2種類の暗号鍵を切り替えて暗号化及び復号化を行う必要がないため、無線基地局及び無線パケット端末にかかる負荷を抑制することができる。

【0089】なお、本実施形態においてブロードキャストパケットをパケット網で転送する様子は、図11に示す第3実施形態の場合に等しい。また、上述した説明では第2実施形態を基にしたパケット転送手順について説明したが、第1実施形態を基にしても良い。その場合には、第3実施形態で説明したように、表1に示す端末情報テーブルを使用するとともに、VLAN-IDと送信元アドレスの対応が端末情報に一致するかどうか確認することになる。

【0090】以上のように、本実施形態によれば、第3実施形態と同様に、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【0091】これに加えて本実施形態では、パケットを転送する際、VLAN-IDに共通する暗号鍵を用いて暗号化しているため、無線基地局は同じVLAN-IDを有する配下の全無線パケット端末に対して、1回の送信でブロードキャストパケット及びマルチキャストパケットを転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制することができる。

【0092】また、VLAN-IDに共通する暗号鍵を用いているため、無線基地局及び無線パケット端末はパケットを受信した時に暗号鍵を切り替えることなく復号することが可能となる。したがって、2種類の暗号鍵を用いる場合に比べて、無線基地局及び無線パケット端末にかかる負荷を抑制することができる。なお、VLAN鍵は端末固有の暗号鍵ではないが、異なるVLAN-IDを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【0093】〔第6実施形態〕この第6実施形態は、請求項1、3、5記載のパケット転送方法および請求項12記載の基地局を適用した場合に相当している。本実施形態では第1実施形態に変形を加えて、VLAN-IDを通信開始時において動的に割り当てるようにしたもの

である。本実施形態におけるパケット網のネットワーク構成、無線基地局の構成、データパケットの改竄検出手順及びパケットの信号フォーマットは、図1、図2、図4及び図5に示した第1実施形態の場合とそれぞれ等しい。

【0094】本実施形態では、VLAN-IDの動的割り当てを実現するためにユーザLAN1-4の各々にあらかじめ固有の名称（以下、「ユーザLAN名」という）を割り当てておく。例えば図1において、LAN#Aには「ユーザLAN#A」を割り当て、LAN#Bには「ユーザLAN#B」を割り当てるようにする。また、本実施形態ではユーザLAN名とVLAN-IDの対応関係を保持するために、無線基地局1-6が表4に示すVLAN-ID割当管理テーブルを記憶している。さらに本実施形態において、端末認証サーバ1-8の保持する端末情報テーブルは表5に示す通りであり、VLAN-IDの代わりにユーザLAN名を使用する点が第1実施形態（表1）と異なっている。

【0095】

【表4】

VLAN-ID割当管理テーブル

ユーザLAN名	VLAN-ID
ユーザLAN#A	VLAN-ID#A
ユーザLAN#B	VLAN-ID#B
⋮	⋮

【0096】

【表5】

端末情報テーブル

端末アドレス	ユーザLAN名	暗号鍵
アドレス#1	ユーザLAN#A	暗号鍵#a
アドレス#2	ユーザLAN#A	暗号鍵#b
アドレス#3	ユーザLAN#B	暗号鍵#c

【0097】本実施形態では図3に示した認証手順に一部変更を加えて図14に示す無線パケット端末の認証手順を採用している。図14に示すように、無線パケット端末1-7は通信開始要求信号を無線基地局1-6へ送信する際に、自分の所属しているユーザLANに割り当てられたユーザLAN名（例えば「ユーザLAN#A」）を含めて送信している（18-1）。無線基地局1-6では、端末認証手段10が送られたユーザLAN名を内部に記憶しておく。次に、第1実施形態と同様に、無線基地局1-6は端末認証サーバ1-8に要求（2-2）を行って端末情報を取得（2-3）してこれを端末情報記憶手段11に記憶し、端末認証用の乱数を暗号化して無線パケット端末1-7に認証要求信号を送信（2-4）し、無線パケット端末1-7が送り返す認

証応答信号(2-5)に基づいて認証を行う。

【0098】この認証によって無線パケット端末1-7が正規の端末と判断された場合、端末認証手段10は無線パケット端末1-7から通知(18-1)されているユーザLAN名にVLAN-IDを割り当てる(18-6)。いま、無線パケット端末1-7から通知された例えばユーザLAN名が「ユーザLAN#A」である場合、端末認証手段10はこのユーザLANに対して例えば「VLAN-ID#A」を割り当て、表4に示すように「ユーザLAN#A」および「VLAN-ID#A」の組をVLAN-ID割当管理テーブルに追加する。次いで、端末認証手段10は認証受付信号を用いて無線パケット端末1-7に通信許可を通知するが、このとき端末認証手段10はいま割り当てたVLAN-ID#Aを無線パケット端末1-7に通知する(18-7)。なお、無線パケット端末1-7が不正端末と判断された場合の処理は第1実施形態と同じである。

【0099】一方、図15は本実施形態におけるパケット転送手順を示している。まず、本実施形態では認証手順として図14に示した認証手順を実行する(19-1)。次に、無線パケット端末1-7はデータパケットを無線基地局1-6に送信するが、その際、VLAN-ID4-3としては先に通知されたVLAN-ID(図14の18-7)を用いる。この後は、第1実施形態と同様にして宛先端末へのデータパケットの転送(5-2)の処理までを行うが、データパケットが改竄されておらず、ユーザLAN名と送信元アドレスの対応が端末情報に一致するかどうか確認する際(19-2)には次に述べる処理を行う。すなわち、無線基地局1-6では、端末アドレス/VLAN-ID比較手段15が、送信元アドレス4-2に対応するユーザLAN名を表5に示す端末情報テーブルから取得し、取得したユーザLAN名に対応するVLAN-IDを表4に示すVLAN-ID割当管理テーブルから検索し、検索されたVLAN-ID割当管理テーブル

端末アドレス	ユーザLAN名	ユーザLAN名	暗号鍵
アドレス#1	ユーザLAN#A	ユーザLAN#B	暗号鍵#a
アドレス#2	ユーザLAN#A	ユーザLAN#B	暗号鍵#b
アドレス#3	ユーザLAN#B	-	暗号鍵#c

【0104】本実施形態における無線パケット端末の認証手順は図16に示すものとなる。図16に示す認証手順と図14(第6実施形態)との相違は、無線パケット端末1-7が通信開始要求信号を無線基地局1-6へ送信する際に、通信相手のユーザLAN名を指定して無線基地局1-6に通知する(20-1)点である。したがって、この後に行われる認証手順は第6実施形態と同じである。

【0105】一方、図17は本実施形態におけるパケット転送手順を示している。本実施形態では、まず認証手

—IDとデータパケット中のVLAN-ID4-3が一致するかどうか判定する。フィルタリング手段16はこの判定結果に基づいて、両者が一致していれば宛先アドレス4-1で指定された宛先端末にデータパケットを転送(5-2)し、両者が一致していなければデータパケットを廃棄する。その後に、無線パケット端末1-7と宛先端末との間で通信が終了したならば、無線基地局1-6では端末認証手段10が表4に示したVLAN-ID割当管理テーブルから「ユーザLAN#A」および「VLAN-ID#A」の組を削除しそれによって、無線パケット端末1-7に割り当てたVLAN-IDを解放する(19-3)。

【0100】以上のように、本実施形態では無線パケット端末1-7に対してVLAN-IDを動的に割り当てているため、限られたVLAN-IDを効率的に再利用することができ、より多くのユーザLANを収容することができる。

【0101】[第7実施形態]この第7実施形態は、請求項1、3、5記載のパケット転送方法および請求項12記載の基地局を適用した場合に相当している。本実施形態は、第6実施形態で説明したVLAN-IDの動的割り当てを第2実施形態に適用したものである。したがって、本実施形態におけるパケット網のネットワーク構成、無線基地局の構成、データパケットの改竄検出手順及びパケットの信号フォーマットは、図1、図2、図4及び図5に示した第1実施形態の場合とそれぞれ等しい。

【0102】本実施形態では、端末認証サーバ1-8が表6に示す端末情報テーブルを記憶している。表5(第6実施形態)と比較した場合、一つの端末アドレスについて、当該端末アドレスを持つパケット端末に通信を許可するユーザLAN名が複数登録されている。

【0103】

【表6】

順として図16に示した手順を実行する(21-1)。次に、無線パケット端末1-7はデータパケットを無線基地局1-6に送信するが、その際、VLAN-ID4-3としては先に通知されたVLAN-ID(図16の18-7)を用いる。この後は、第2実施形態と同様にして宛先端末へのデータパケットの転送(6-2)の処理までを行うが、データパケットが改竄されておらず、ユーザLAN名と送信元アドレスの対応が端末情報に登録済みかどうか確認する際(21-2)には次に述べる処理を行う。すなわち、無線基地局1-6において、端

末アドレス/VLAN-ID比較手段15は、受信パケットに含まれるVLAN-ID4-3に対応するユーザLAN名を表4に示すVLAN-ID割当管理テーブルから検索し、検索されたユーザLAN名と受信パケットに含まれる送信元アドレス4-2の組が、表6に示す端末情報テーブル中の端末アドレスとユーザLAN名の複数の組の中に存在するかどうかを調べ、この組が端末情報テーブルに存在していなければ上記対応が端末情報に未登録であると判断する。一方、この組が端末情報テーブルに存在する場合、端末アドレス/VLAN-ID比較手段15は当該ユーザLAN名に割り当ててあるVLAN-IDを表4に示すVLAN-ID割当管理テーブルから取得し、取得したVLAN-IDとパケット中のVLAN-ID4-3が一致するかどうか調べ、一致していれば上記対応が端末情報に登録済みであると判断し、一致していなければ上記対応が端末情報に未登録であると判断する。フィルタリング手段16は、この判断結果に基づいて上記対応が端末情報に登録済みであれば宛先アドレス4-1で指定された宛先端末にデータパケットを転送(6-2)し、上記対応が端末情報に未登録であればデータパケットを廃棄する。その後、無線パケット端末1-7と宛先端末の間で通信が終了したならば、第6実施形態と同様にして、端末認証手段10は無線パケット端末1-7に割り当てたVLAN-IDを解放する(21-3)。

【0106】〔第8実施形態〕この第8実施形態は、請求項1、2、5記載のパケット転送方法および請求項1記載の基地局を適用した場合に相当している。これまで説明した各実施形態では、端末アドレスとしてMACアドレスを用い、ユーザLANに対してVLAN-IDを割り当てるようにしていた。これに対して、本実施形態では端末アドレスとしてIPアドレスを用いるとともに、ユーザLANには各ユーザLAN1-4に対して固有のネットワークアドレスをあらかじめ割り当てておく。前述したようにIPアドレスは図18に示す構成をしているが、本実施形態ではこのIPアドレスに含まれるネットワークアドレス部をVLAN-IDの代わりに用いる。つまり、本実施形態においてはデータパケット中の宛先アドレス4-1の上位ビットを抽出することでネットワークアドレスが得られることになる。したがって、図5に示したVLAN-ID4-3は不要となり、本実施形態における信号フォーマットは図19に示すものとなる。

【0107】また、本実施形態における端末情報テーブルは表7に示すものとなり、表1で使用されていたVLAN-IDの代わりにネットワークアドレスが使用される。さらに、本実施形態における無線パケット端末1-7は、自分の所属するユーザLAN1-4のネットワークアドレスをそれぞれ端末認証サーバ1-8にあらかじめ登録している。なお、本実施形態におけるパケット網

のネットワーク構成、無線基地局の構成、無線パケット端末の認証手順及びデータパケットの改竄検出手順は、図1～図4に示した第1実施形態の場合とそれぞれ等しい。

【0108】

【表7】

端末情報テーブル

端末アドレス	ネットワークアドレス	暗号鍵
アドレス#1	ネットワークアドレス#A	暗号鍵#a
アドレス#2	ネットワークアドレス#A	暗号鍵#b
アドレス#3	ネットワークアドレス#B	暗号鍵#c

【0109】図20は本実施形態におけるパケット転送手順を示しており、図6(第1実施形態)に示したパケット転送手順とは以下の点が相違する。すなわち、無線基地局1-6では、パケット改竄検出手段14が受信したデータパケット(5-1)の改竄を検出しなかった場合、端末アドレス/VLAN-ID比較手段15は、受信したデータパケットの宛先アドレス4-1からネットワークアドレス部を抽出し、送信元アドレス4-2に基づいて表7に示した端末情報テーブルから無線パケット端末1-7の所属するユーザLANのネットワークアドレスを取得して、これら2つのネットワークアドレスが一致するかどうかを確認する(24-1)。その後、フィルタリング手段16は送られた確認結果に基づいて、両ネットワークアドレスが一致していれば第1実施形態と同様に宛先アドレス4-1で指定された宛先端末にデータパケットを転送する(5-2)。一方、両ネットワークアドレスが一致していなければ、フィルタリング手段16はデータパケットを廃棄する。

【0110】以上のように、本実施形態では、第1実施形態のようにデータパケット中にVLAN-IDのような余分なフィールドを設ける必要がない。

【0111】〔第9実施形態〕この第9実施形態は、請求項1、2、5記載のパケット転送方法および請求項1記載の基地局を適用した場合に相当している。本実施形態は、第8実施形態で説明したネットワークアドレスの使用を第2実施形態に適用したものである。本実施形態においても、ユーザLAN1-4に対して各ユーザLANに固有のネットワークアドレスをあらかじめ割り当てておく。また、本実施形態における端末情報テーブルは表8に示す通りであって、表2で使用されていたVLAN-IDの代わりにネットワークアドレスが使用されている。なお、本実施形態におけるパケット網のネットワーク構成、無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図1～図4及び図19に示したものとそれぞれ等しい。

【0112】

【表8】

端末情報テーブル

端末アドレス	ネットワークアドレス	ネットワークアドレス	暗号鍵
アドレス#1	ネットワークアドレス#A	ネットワークアドレス#B	暗号鍵#a
アドレス#2	ネットワークアドレス#A	ネットワークアドレス#B	暗号鍵#b
アドレス#3	ネットワークアドレス#B	—	暗号鍵#c

【0113】図21は本実施形態におけるパケット転送手順を示しており、図7（第2実施形態）に示したパケット転送手順とは以下の点が相違する。すなわち、無線基地局1-6では、パケット改竄検出手段14が受信したデータパケット（6-1）の改竄を検出なかった場合、端末アドレス/VLAN-ID比較手段15は、受信したデータパケットの宛先アドレス4-1からネットワークアドレス部を抽出し、送信元アドレス4-2に基づいて無線パケット端末1-7が通信を許されているユーザLANに割り当てられている全てのネットワークアドレスを表8に示した端末情報テーブルから取得する。次いで、端末アドレス/VLAN-ID比較手段15は、取得したネットワークアドレスの中に宛先アドレス4-1から抽出されたネットワークアドレスと一致するものが登録されているかどうかを確認する。フィルタリング手段16は送られた確認結果に基づいて、一致するネットワークアドレスが存在していれば宛先アドレス4-1で指定された宛先端末にデータパケットを転送（6-2）し、一致するネットワークが全く無ければデータパケットを廃棄する。

【0114】以上のように、本実施形態においても、第1実施形態のようにデータパケット中にVLAN-IDのような余分なフィールドを設ける必要がない。

【0115】〔第10実施形態〕この第10実施形態は、請求項1、2、4、5、8記載のパケット転送方法および請求項11、13記載の基地局を適用した場合に相当している。本実施形態は、第8実施形態で説明したネットワークアドレスの使用を第3実施形態に適用したものである。本実施形態においても、ユーザLAN1-4には各ユーザLANに固有のネットワークアドレスをあらかじめ割り当てておく。本実施形態におけるパケット網のネットワーク構成は図8に示した第3実施形態の場合と等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図2～図4及び図19に示したものとそれぞれ等しい。また、端末認証サーバ7-8には表9に示すVLAN情報テーブルが設けられており、VLAN-IDの代わりにネットワークアドレスを使用している点で表3（第3実施形態）と相違している。なお、本実施形態においても、第3実施形態と同様に、無線パケット網が各無線パケット端末7-7にVLAN鍵をあらかじめ通知しておく。

【0116】

【表9】

VLAN情報テーブル

ネットワークアドレス	VLAN鍵
ネットワークアドレス #A	VLAN鍵#a
ネットワークアドレス #B	VLAN鍵#b

【0117】図22は本実施形態におけるパケット転送手順を示しており、図9に示した第3実施形態の手順とは以下の点が相違する。まず、受信したデータパケット（8-1）の改竄が検出されなかった場合、第9実施形態と同様に、端末アドレス/VLAN-ID比較手段15は、受信したデータパケットの宛先アドレス4-1から抽出されるネットワークアドレスが、無線パケット端末7-7に対して通信が許可されている複数のユーザLAN1-4に割り当てたネットワークアドレスの中に登録されているかどうかを確認する（26-1）。そしてフィルタリング手段16はこの確認結果に応じてパケットを転送する（8-2）か廃棄するかを決定する。

【0118】ここで、データパケットを転送する際（8-2）に、宛先端末がユーザLAN7-4と接続している場合、各中継ノード7-9はデータパケット中の宛先アドレス4-1に応じて次の送信ポートを選択してゲートウェイ7-3へデータパケットを転送する。ゲートウェイ7-3は宛先アドレス4-1から抽出されるネットワークアドレスに応じてゲートウェイ7-1又はゲートウェイ7-2を選択して、データパケットをユーザLAN7-4から宛先端末に転送する。一方、宛先端末が無線パケット網と接続している場合は、第3実施形態と同様に、各中継ノード7-9は宛先アドレス4-1に応じて次の送信ポートを選択して、ゲートウェイを介することなくパケットを宛先端末へ転送する。

【0119】本実施形態におけるブロードキャストパケットの転送手順は基本的に第3実施形態（図10）と同様であって、VLAN-IDの代わりに宛先アドレスから抽出されるネットワークアドレスを用いて経路選択が行われる点が相違している。

【0120】以上のように、本実施形態においても、第1実施形態のようにデータパケット中にVLAN-IDのような余分なフィールドを設ける必要がない。なお、ここではネットワークアドレスの使用を第3実施形態へ適用した場合について説明したが、第3実施形態と第4～第5実施形態とでは無線パケット端末7-7から無線基地局7-6へデータパケットを送信する際の暗号鍵の

使い方が異なるだけである。したがって、これら第 4 ～ 第 5 実施形態においても V L A N - I D の代わりにネットワークアドレスを使用することができる。

【 0 1 2 1 】 【 第 1 1 実施形態 】 この第 1 1 実施形態は、請求項 1、6 記載のバケット転送方法を適用した場合に相当している。

【 0 1 2 2 】 本実施形態におけるバケット網の構成、無線基地局の構成、無線バケット端末の認証手順及びデータバケットの改竄検出手順は、図 1 ～ 図 4 に示した第 1 実施形態の場合とそれぞれ等しい。

【 0 1 2 3 】 表 1 0 は、本実施形態における端末情報テーブルを示しており、端末アドレスと、端末認証に必要な情報としての暗号鍵とで構成されている。

【 0 1 2 4 】

【 表 1 0 】

第 1 2 実施形態における端末情報テーブル

端末アドレス	暗号鍵
アドレス#1	暗号鍵#a
アドレス#2	暗号鍵#b
アドレス#3	暗号鍵#c

【 0 1 2 5 】 各ユーザ LAN 1 - 4 に接続するゲートウェイ 1 - 1、1 - 2 は、それぞれ許可アドレス情報を許可アドレステーブルに持っている。表 1 1 はゲートウェイ 1 - 1 の許可アドレステーブルを示しており、表 1 2 はゲートウェイ 1 - 2 の許可アドレステーブルを示している。ゲートウェイ 1 - 1、1 - 2 は、送信元アドレス 4 - 2 が各ゲートウェイの許可アドレステーブルに登録されているデータバケットだけをユーザ LAN 1 - 4 に転送する。

【 0 1 2 6 】

【 表 1 1 】

ゲートウェイ 1 - 1、7 - 1 の許可アドレステーブル

許可アドレス
アドレス#1
アドレス#2
—

【 0 1 2 7 】

【 表 1 2 】

ゲートウェイ 1 - 2、7 - 2 の許可アドレステーブル

許可アドレス
アドレス#3
—
—

【 0 1 2 8 】 また、本実施形態における無線バケット網のバケットの信号フォーマットは、第 8 実施形態で説明した図 1 9 のものと同じであって、宛先アドレス 4 - 1 と送信元アドレス 4 - 2 をヘッダ情報として持ってお

り、ユーザデータ 4 - 4 は暗号化される。

【 0 1 2 9 】 図 2 3 は、本実施形態におけるバケット転送手順を示している。無線基地局 1 - 6 では、端末認証手段 1 0 が通信開始時に無線バケット端末 1 - 7 に対する認証を行い、当該バケット端末が正規の端末の場合は暗号通信を開始する。なお、この認証に際して端末認証手段 1 0 は端末認証サーバ 1 - 8 から端末情報を得る。次に、無線バケット端末 1 - 7 は暗号化されたデータバケットを無線基地局 1 - 6 に送信する (1 4 - 1)。無線基地局 1 - 6 ではバケット復号化手段 1 3 がデータバケットを復号化して、バケット改竄検出手段 1 4 が受信データバケット (1 4 - 1) の改竄を検出した場合はこの受信データバケットを廃棄する。なお、これまでの手順は第 1 実施形態 (図 6) と同じである。一方、改竄が検出されない場合、端末アドレス / V L A N - I D 比較手段 1 5 は第 1 実施形態のように V L A N - I D と送信元アドレスとの対応を確認することはせず、受信データバケットをそのままフィルタリング手段 1 6 に送出し、フィルタリング手段 1 6 は宛先アドレス 4 - 1 で指定された宛先端末にデータバケットを転送する (1 4 - 2)。この時、宛先端末がユーザ LAN 1 - 4 と接続していれば、データバケットはゲートウェイ 1 - 3 からゲートウェイ 1 - 1 又はゲートウェイ 1 - 2 を介してユーザ LAN 1 - 4 に転送される。その際、選択されたゲートウェイはデータバケット中の送信元アドレス 4 - 2 を確認し、当該アドレスが選択されたゲートウェイの許可アドレステーブルに登録済みであればデータバケットをユーザ LAN 1 - 4 に転送し、未登録であれば当該データバケットを廃棄する。一方、宛先端末が無線バケット網と接続している場合、データバケットはゲートウェイを介することなく宛先端末に転送される。

【 0 1 3 0 】 以上のように、本実施形態では、通信開始時に端末認証することによって、無線バケット端末を特定可能であり、未知の端末や端末アドレスを偽造した端末からの不正アクセスを防止することができる。また、暗号化してバケットを転送することにより、不正な端末が認証された正規の端末になりすますことを防止可能であり、なりすまし端末による不正アクセスを防止することができる。さらに、暗号の復号時に改竄を検出してバケットを廃棄することにより、改竄されたバケットの転送を防止可能であり、改竄データによる通信の妨害と無線バケット網のトラヒック増加を防止することができる。加えて、ゲートウェイが宛先アドレスと送信元アドレスに応じてバケットの転送を許可することで、認証されたバケット端末が通信の許可されていないユーザ LAN にアクセスするのを防止可能であり、他ユーザ LAN に所属している端末からの不正アクセスを防止することができる。

【 0 1 3 1 】 【 第 1 2 実施形態 】 この第 1 2 実施形態は、請求項 1、7、8 記載のバケット転送方法を適用し

た場合に相当している。

【0132】本実施形態におけるパケット網の構成は図8に示す第3実施形態の構成に等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図2～図5に示した第1実施形態の場合とそれぞれ等しい。

【0133】第3実施形態と同様に、VLAN-IDは各ユーザLAN7-4に固有の値があらかじめ割り当てられている。

【0134】端末認証サーバ7-8は第3実施形態と同様に端末情報テーブルとVLAN情報テーブルを有している。本実施形態におけるVLAN情報テーブルは、表3に示す第3実施形態におけるVLAN情報テーブルに等しい。本実施形態では、VLAN鍵がブロードキャストパケット及びマルチキャストパケットの暗号化に使用される。なお、無線パケット網は各無線パケット端末7-7にVLAN鍵をあらかじめ通知しておく。

【0135】本実施形態における端末情報テーブルは、表10に示す第11実施形態における情報テーブルと等しい。この端末情報テーブルに登録した暗号鍵（端末鍵）は、端末認証及びユニキャストパケットの暗号化に用いられる。なお、無線パケット網は各無線パケット端末7-7に端末鍵をあらかじめ通知しておく。

【0136】各ユーザLAN7-4に接続するゲートウェイ7-1、7-2は、第11実施形態におけるゲートウェイ1-1、1-2と同様に、許可アドレス情報を表11、表12に示した許可アドレステーブルに持っている。

【0137】図24は、本実施形態におけるパケット転送手順を示している。第3実施形態と同様に、無線基地局7-6では端末認証手段10が通信開始時に無線パケット端末7-7に対する認証を行い、当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証手段10が端末認証サーバ7-8から端末情報と共にVLAN情報を得るのも第3実施形態と同じである。次に、無線パケット端末7-7は第3実施形態と同様にパケットに応じた暗号鍵としてVLAN鍵又は端末鍵を選択し、暗号化されたデータパケットを無線基地局7-6に送信する（15-1）。無線基地局7-6は第3実施形態と同様にパケットに応じた復号鍵を選択してデータパケットを復号化する。そして、パケット改竄検出手段14が受信データパケット（15-1）の改竄を検出した場合はこの受信データパケットを廃棄する。一方、改竄が検出されない場合、端末アドレス/VLAN-ID比較手段15は第3実施形態のようにVLAN-IDと送信元アドレスとの対応を確認することはせず、受信データパケットをそのままフィルタリング手段16に送出し、フィルタリング手段16は宛先アドレス4-1で指定される宛先端末に転送するために

データパケットを無線パケット網へ送信する（15-2）。この時、宛先端末がユーザLAN7-4と接続している場合、各中継ノード7-9はデータパケット中の宛先アドレス4-1に応じて次の送信ポートを選択してゲートウェイ7-3へデータパケットを転送する。ゲートウェイ7-3は宛先アドレス4-1から抽出されるネットワークアドレスに応じてゲートウェイ7-1又はゲートウェイ7-2を選択し、選択されたゲートウェイに接続するユーザLAN7-4から宛先端末にデータパケットを転送する（15-3）。その際、選択されたゲートウェイはデータパケット中の送信元アドレス4-2を確認し、当該アドレスが選択されたゲートウェイの許可アドレステーブルに登録済みであればデータパケットをユーザLAN7-4に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合は、第3実施形態と同様に、各中継ノード7-9は宛先アドレス4-1に応じて次の送信ポートを選択して、ゲートウェイを介することなくデータパケットを宛先端末へ転送する。

【0138】本実施形態におけるブロードキャストパケットの転送手順は、図10に示す第3実施形態の場合と等しい。本実施形態では、暗号化にVLAN鍵を用いているため、第3実施形態と同様に、VLAN-IDの同じパケット端末は、ブロードキャストパケット及びマルチキャストパケットの復号が可能である。

【0139】また、本実施形態においてブロードキャストパケットをパケット網が転送する様子は、図11に示す第3実施形態の場合と等しい。

【0140】以上のように、本実施形態によれば、第11実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、VLAN-IDにより次の中継ノードを選択してパケットを転送するため、同じVLAN-IDを用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり、最適な経路選択で転送することが可能であって、転送遅延時間、トラヒック、ゲートウェイの処理負荷の増加を防止することができる。また、ブロードキャストパケット又はマルチキャストパケットを転送する際は、VLAN-IDに共通する暗号鍵を用いて暗号化しているため、無線基地局は同じVLAN-IDを持つ配下の全無線パケット端末に対して1回の送信でこれらパケットを転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、

転送遅延時間、基地局の負荷をそれぞれ抑制することができる。なお、VLAN鍵は端末固有の暗号鍵ではないが、異なるVLAN-IDを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【0141】〔第13実施形態〕この第13実施形態は、請求項1、7、9記載のパケット転送方法を適用した場合に相当している。

【0142】本実施形態におけるパケット網の構成は図8に示す第3実施形態の構成に等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図2～図5に示した第1実施形態の場合とそれぞれ等しい。

【0143】第3実施形態と同様に、VLAN-IDは各ユーザLANに固有の値があらかじめ割り当てられている。端末認証サーバ7-8は第3実施形態と同様に端末情報テーブルとVLAN情報テーブルを有している。本実施形態におけるVLAN情報テーブルは、表3に示す第3実施形態におけるVLAN情報テーブルに等しい。

【0144】本実施形態において、VLAN鍵は無線基地局7-6がブロードキャストパケット及びマルチキャストパケットを暗号化するとき使用される。なお、無線パケット網は各無線パケット端末7-7にVLAN鍵をあらかじめ通知しておく。

【0145】また、本実施形態における端末情報テーブルは表10に示す第11実施形態の端末情報テーブルと等しい。この端末情報テーブルに登録した暗号鍵（端末鍵）は、端末認証時、ユニキャストパケットの暗号化時、ならびに、無線パケット端末7-7によるブロードキャスト及びマルチキャストパケットの暗号化時においてそれぞれ用いられる。なお、無線パケット網は各無線パケット端末7-7に端末鍵をあらかじめ通知しておく。

【0146】ゲートウェイ7-1、7-2は第11実施形態におけるゲートウェイ1-1、1-2と同様に、表11、表12に示す許可アドレステーブルをそれぞれ有している。

【0147】図25は、本実施形態におけるパケット転送手順を示している。第3実施形態と同様に、無線基地局7-6では端末認証手段10が通信開始時に無線パケット端末7-7に対する認証を行い、当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証手段10が端末認証サーバ7-8から端末情報と共にVLAN情報を得るのも第3実施形態と同じである。次に、無線パケット端末7-7は第4実施形態と同様にユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なく端末鍵を用いてデータパケットを暗号化して無線基地局7-6に送信する（16-1）。無線基地局7-6では、パ

ケット復号化手段13がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなく端末鍵を用いてデータパケットを復号化する。これ以後は、第12実施形態と同様に、無線基地局7-6は受信したデータパケットが改竄されていればパケットを廃棄し、改竄されていない場合は、VLAN-IDと送信元アドレスとの対応を確認することなく、第12実施形態と同様にして宛先アドレス4-1で指定される宛先端末までデータパケットを転送する（16-3）。すなわち、宛先端末がユーザLAN7-4と接続しているならば、データパケットは各中継ノード7-9、ゲートウェイ7-3、ゲートウェイ7-1又はゲートウェイ7-2、ユーザLAN7-4を経て宛先端末に転送される。その際、ゲートウェイ7-1又は7-2はデータパケット（16-2）の送信元アドレス4-2が許可アドレステーブルに登録済みであればデータパケットをユーザLAN7-4に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合、データパケットはゲートウェイを介することなく宛先端末へ転送される。

【0148】また、本実施形態においてブロードキャストパケットをパケット網が転送する様子は図11に示す第3実施形態の場合に等しい。

【0149】本実施形態によれば、第11実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、VLAN-IDにより次の中継ノードを選択してパケットを転送するため、同じVLAN-IDを用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり、最適な経路選択で転送することが可能であって、転送遅延時間、トラヒック、ゲートウェイの処理負荷の増加を防止することができる。また、無線基地局が送信するブロードキャストパケット及びマルチキャストパケットの暗号化の際にはVLAN鍵を用いるため、VLAN-IDの同じパケット端末は暗号の復号が可能である。また、無線基地局がブロードキャストパケット又はマルチキャストパケットを転送する際は、VLAN-IDに共通する暗号鍵を用いて暗号化しているため、無線基地局は同じVLAN-IDを持つ配下の全無線パケット端末に対して1回の送信でこれらパケットを転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制することができる。さらに、無線パケット端

末は、送信するブロードキャストパケット及びマルチキャストパケットの暗号化に際して、ユニキャストパケット用の暗号鍵である端末鍵を用いている。そのため、第 1 2 実施形態などとは異なり、無線基地局はパケットの受信時に 2 種類の暗号鍵を切り替えることなく暗号を復号することが可能となる。したがって、ブロードキャストパケット及びマルチキャストパケット用の暗号鍵を用いて暗号化して送信する場合に比べて、無線基地局の負荷を抑制することができる。

【0150】〔第 1 4 実施形態〕この第 1 4 実施形態は、請求項 1, 7, 10 記載のパケット転送方法を適用した場合に相当している。

【0151】本実施形態におけるパケット網の構成は図 8 に示す第 3 実施形態の構成に等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図 2 ～図 5 に示した第 1 実施形態の場合とそれぞれ等しい。

【0152】第 3 実施形態と同様に、VLAN-ID は各ユーザ LAN に対して固有の値があらかじめ割り当てられている。端末認証サーバ 7-8 は第 3 実施形態と同様に端末情報テーブルと VLAN 情報テーブルを有している。本実施形態における VLAN 情報テーブルは、表 3 に示す第 3 実施形態における VLAN 情報テーブルに等しい。本実施形態では、第 5 実施形態と同様に、VLAN 鍵はパケットを暗号化するときを使用される。なお、無線パケット網は各無線パケット端末 7-7 に VLAN 鍵をあらかじめ通知しておく。

【0153】本実施形態における端末情報テーブルは表 10 に示した第 1 1 実施形態の端末情報テーブルと等しい。また、端末情報テーブルに登録した暗号鍵としては、各端末が所属するユーザ LAN 7-4 の VLAN 鍵を用いる。

【0154】ゲートウェイ 7-1, 7-2 は第 1 1 実施形態におけるゲートウェイ 1-1, 1-2 と同様に、それぞれ表 1 1, 表 1 2 に示す許可アドレステーブルを有している。

【0155】図 2 6 は、本実施形態におけるパケット転送手順を示している。第 3 実施形態と同様に、無線基地局 7-6 では端末認証手段 10 が通信開始時に無線パケット端末 7-7 に対する認証を行い、当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証手段 10 が端末認証サーバ 7-8 から端末情報と共に VLAN 情報を得るのも第 3 実施形態と同じである。次に、無線パケット端末 7-7 は第 5 実施形態と同様にユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なく VLAN 鍵を用いてデータパケットを暗号化して無線基地局 7-6 に送信する (17-1)。無線基地局 7-6 では、パケット復号化手段 13 がユニキャストパケット／

ブロードキャストパケット／マルチキャストパケットを区別することなく VLAN 鍵を用いてデータパケットを復号化する。これ以後は、第 1 2 実施形態と同様に、無線基地局 7-6 は受信したデータパケットが改竄されていればパケットを廃棄し、改竄されていない場合は、VLAN-ID と送信元アドレスとの対応を確認することなく、第 1 2 実施形態と同様にして宛先アドレス 4-1 で指定される宛先端末までデータパケットを転送する

(17-3)。すなわち、宛先端末がユーザ LAN 7-4 と接続しているならば、データパケットは各中継ノード 7-9, ゲートウェイ 7-3, ゲートウェイ 7-1 又はゲートウェイ 7-2, ユーザ LAN 7-4 を経て宛先端末に転送される。その際、ゲートウェイ 7-1 又は 7-2 はデータパケット (17-2) の送信元アドレス 4-2 が許可アドレステーブルに登録済みであればデータパケットをユーザ LAN 7-4 に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合、データパケットはゲートウェイを介することなく宛先端末へ転送される。

【0156】本実施形態においてブロードキャストパケットをパケット網が転送する様子は、図 1 1 に示す第 3 実施形態の場合と等しい。

【0157】以上のように、本実施形態によれば、第 1 1 実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、VLAN-ID により次の中継ノードを選択してパケットを転送するため、同じ VLAN-ID を用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり、最適な経路選択で転送することが可能であって、転送遅延時間、トラヒック、ゲートウェイの処理負荷の増加を防止することができる。また、本実施形態では、暗号化に VLAN 鍵のみを用いるようにして端末鍵を用いないため、VLAN-ID の同じパケット端末はブロードキャスト及びマルチキャストパケットの暗号を復号することが可能である。また、VLAN-ID に共通する暗号鍵を用いているため、無線基地局及び無線パケット端末はパケット受信時に 2 種類の暗号鍵を切り替えて暗号化及び復号する必要がない。したがって、2 種類の暗号鍵を用いる場合に比べて、無線基地局及び無線パケット端末の負荷を抑制することができる。また、パケットを転送する際は、VLAN-ID に共通する暗号鍵を用いて暗号化しているため、無線基地局は同じ VLAN-ID を持つ配下の全無線パケット端末に対して 1 回の送信でこれらパケットを

転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制することができる。なお、VLAN鍵は端末固有の暗号鍵ではないが、異なるVLAN-IDを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【0158】〔第15実施形態〕上述した各実施形態では本発明を無線パケット網へ適用した場合について説明してきたが、本発明は無線パケット網に限らず有線パケット網に適用しても良い。図27は、前述した第1実施形態を有線パケット網で実現した場合のネットワーク構成を示している。同図では、無線パケットバックボーン網1-5と同等の機能を有するパケットバックボーン網27-5、無線／有線の違いを除いて無線基地局1-6と同等の機能を有するアクセスサーバ（有線接続装置）27-6、および無線／有線の違いを除いて無線パケット端末1-7と同等の機能を有するパケット端末27-7がそれぞれ設けられている。これら以外の構成は全て第1実施形態（図1）と同じである。本実施形態によるパケット転送手順は、アクセスサーバ27-6とパケット端末27-7の間を含めた全ての通信が有線で行われる点を除けば、第1実施形態と全く同じになる。また、図8に示したネットワーク構成を用いる場合にも、無線パケットバックボーン網7-5、無線基地局7-6、無線パケット端末7-7をそれぞれパケットバックボーン網27-5、アクセスサーバ27-6、パケット端末27-7に置き換えれば良い。したがって、上述した全ての実施形態に対して有線パケット網のネットワーク構成を適用することができる。

【0159】以上述べた実施形態は全て本発明を例示的に示すものであって限定的に示すものではなく、本発明は他の種々の変形態様及び変更態様で実施することができる。従って本発明の範囲は特許請求の範囲及びその均等範囲によってのみ規定されるものである。

【0160】例えば、上記各実施形態では、パケット網への入口である無線基地局（あるいはアクセスサーバ）が端末認証やパケット改竄検出などを行うことによって、最も効率的な転送を実現することができる。しかしながら、パケット網の構成によっては無線基地局を統括する制御局などが設けられている場合もあり、そうした場合には、この制御局が端末認証やパケット改竄検出を行うようにしても良い。

【0161】

【発明の効果】以上説明したように、本発明によれば、通信開始時に端末認証することによってパケット端末を特定可能であり、未知の端末や端末アドレスを偽造した端末からの不正アクセスを防止する効果が得られる。また、暗号化してパケットを転送することにより、不正な端末が認証された正規の端末になりすますことを防止可

能であり、なりすまし端末による不正アクセスを防止する効果が得られる。さらに、暗号の復号時に改竄を検出してパケットを廃棄することにより、改竄されたパケットの転送を防止可能であり、改竄データによる通信の妨害とパケット網のトラヒック増加を防止する効果が得られる。

【0162】従って、送信元アドレスを偽造することによりデータ網（ユーザLAN）へ不正にアクセスできる問題を解決し、あらかじめ登録した端末に対してだけ特定のデータ網との通信を許可するパケット転送方法を提供することが可能となる。また、パケットの転送遅延時間、トラヒック、ゲートウェイの負荷が増加する問題を解決し、最適な経路選択が可能でなおかつ効率的なパケット転送方法を提供することが可能となる。

【0163】また、請求項2、3、11又は12記載の発明によれば、識別子又はユーザLAN名と送信元アドレスの対応を確認することにより、認証された端末が自分が接続の許可されていない（あるいは自分の属していない）データ網にアクセスすることを防止可能であり、あるデータ網に接続を許可されている（あるいは所属している）端末から他データ網への不正アクセスを防止する効果が得られる。さらにまた、1パケット端末あたり複数の識別子又はユーザLAN名を登録することにより、1つのパケット端末で複数のデータ網にアクセスすることが可能であり、ユーザへのサービス性が向上するという効果が得られる。

【0164】また、請求項4又は7記載の発明によれば、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、パケット端末が他のパケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であり、転送遅延時間の増加を防止する効果が得られる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、識別子に応じて次の中継ノードを選択してパケットを転送するため、同じ識別子を用いて通信している全てのパケット端末に対してゲートウェイからユニキャスト転送する必要がない。したがって、最適な経路選択でパケットを転送することが可能であり、転送遅延時間、トラヒック、ゲートウェイの処理負荷の増加をそれぞれ防止する効果が得られる。

【0165】また、請求項6記載の発明によれば、ゲートウェイが宛先アドレスと送信元アドレスに応じてパケットの転送を許可することで、認証されたパケット端末が通信の許可されていないユーザLANにアクセスすることを防止可能であり、他ユーザLANに所属しているパケット端末からの不正アクセスを防止する効果が得られる。

【0166】また、請求項8又は13記載の発明によれば、識別子が同じであれば共通の暗号鍵を用いてブロードキャストパケット及びマルチキャストパケットを暗号

化しているため、基地局は同一の識別子を持つ配下の全バケット端末に対して1回の送信でこれらバケットを転送することが可能となる。したがって、各バケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷を抑制する効果が得られる。

【0167】また、請求項9又は14記載の発明によれば、基地局がブロードキャストバケット及びマルチキャストバケットを転送する際には、識別子に共通する暗号鍵を用いて暗号化している。このため、基地局は同じ識別子を持つ配下の全バケット端末に対して1回の送信でこれらバケットを転送することが可能となる。したがって、各バケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制する効果が得られる。また、バケット端末がブロードキャストバケット及びマルチキャストバケットを転送する際には、ユニキャストバケット用の暗号鍵を用いて暗号化している。したがって、基地局はバケット端末からバケットを受信した時に暗号鍵を切り替えることなく復号することが可能となり、ブロードキャストバケット及びマルチキャストバケット用の暗号鍵を用いて暗号化して送信する場合に比べて、基地局にかかる負荷を抑制する効果が得られる。

【0168】また、請求項10又は15記載の発明によれば、バケットを転送する際、識別子に共通の暗号鍵を用いて暗号化しているため、基地局は同じ識別子を有する配下の全バケット端末に対して1回の送信でブロードキャストバケット及びマルチキャストバケットを転送することが可能となる。したがって、各バケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制する効果が得られる。また、識別子に共通する暗号鍵を用いているため、基地局及びバケット端末はバケットの受信時において暗号鍵を切り替えることなく復号することが可能となる。したがって、2種類の暗号鍵を用いる場合に比べて、基地局及びバケット端末にかかる負荷を抑制する効果が得られる。

【図面の簡単な説明】

【図1】 本発明の第1実施形態における無線バケット通信のネットワーク構成を示すブロック図である。

【図2】 本発明の各実施形態における無線基地局の構成を示すブロック図である。

【図3】 本発明の第1実施形態における無線バケット通信の認証手順を示す図である。

【図4】 同実施形態におけるデータバケットの改竄検出手順を示す図である。

【図5】 同実施形態におけるバケットの信号フォーマットを示す図である。

【図6】 同実施形態におけるバケット転送手順を示す図である。

【図7】 本発明の第2実施形態におけるバケット転送手順を示す図である。

【図8】 本発明の第3実施形態における無線バケット通信のネットワーク構成を示すブロック図である。

【図9】 同実施形態におけるバケット転送手順を示す図である。

【図10】 同実施形態におけるブロードキャストバケットの転送手順を示す図である。

【図11】 同実施形態におけるブロードキャストバケットの転送の様子を示す図である。

【図12】 本発明の第4実施形態におけるバケット転送手順を示す図である。

【図13】 本発明の第5実施形態におけるバケット転送手順を示す図である。

【図14】 本発明の第6実施形態における無線バケット通信の認証手順を示す図である。

【図15】 同実施形態におけるバケット転送手順を示す図である。

【図16】 本発明の第7実施形態における無線バケット通信の認証手順を示す図である。

【図17】 同実施形態におけるバケット転送手順を示す図である。

【図18】 IPアドレスの構成を示す図である。

【図19】 本発明の第8実施形態におけるバケットの信号フォーマットを示す図である。

【図20】 同実施形態におけるバケット転送手順を示す図である。

【図21】 本発明の第9実施形態におけるバケット転送手順を示す図である。

【図22】 本発明の第10実施形態におけるバケット転送手順を示す図である。

【図23】 本発明の第11実施形態におけるバケット転送手順を示す図である。

【図24】 本発明の第12実施形態におけるバケット転送手順を示す図である。

【図25】 本発明の第13実施形態におけるバケット転送手順を示す図である。

【図26】 本発明の第14実施形態におけるバケット転送手順を示す図である。

【図27】 本発明の第15実施形態における有線バケット通信のネットワーク構成を示すブロック図である。

【符号の説明】

1-1、1-2、1-3、7-1、7-2、7-3 ゲートウェイ

1-4、7-4 ユーザLAN

1-5、7-5 無線バケットバックボーン網

1-6、7-6、7-6a~7-6c 無線基地局

1-7、7-7、7-7a~7-7c 無線バケット端末

50 1-8、7-8 端末認証サーバ

1-10、7-10 中継路

4-1 宛先アドレス

4-2 送信元アドレス

4-3 VLAN-ID

4-4 ユーザデータ

7-9、7-9a~7-9c 中継ノード

10 端末認証手段

11 端末情報記憶手段

12 パケット暗号化手段

13 パケット復号化手段

14 パケット改竄検出手段

15 端末アドレス/VLAN-ID比較手段

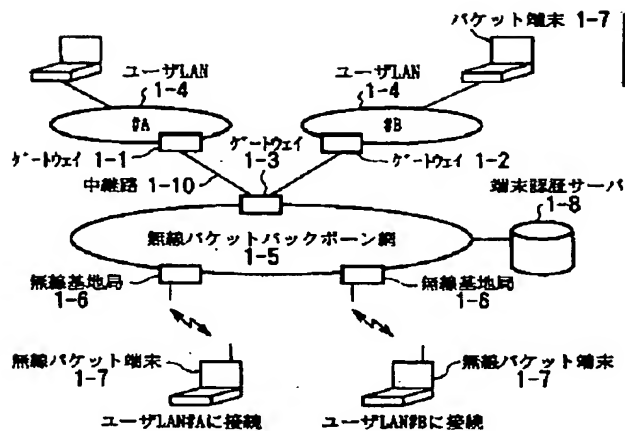
16 フィルタリング手段

27-5 パケットバックボーン網

27-6 アクセスサーバ(有線接続装置)

27-7 パケット端末

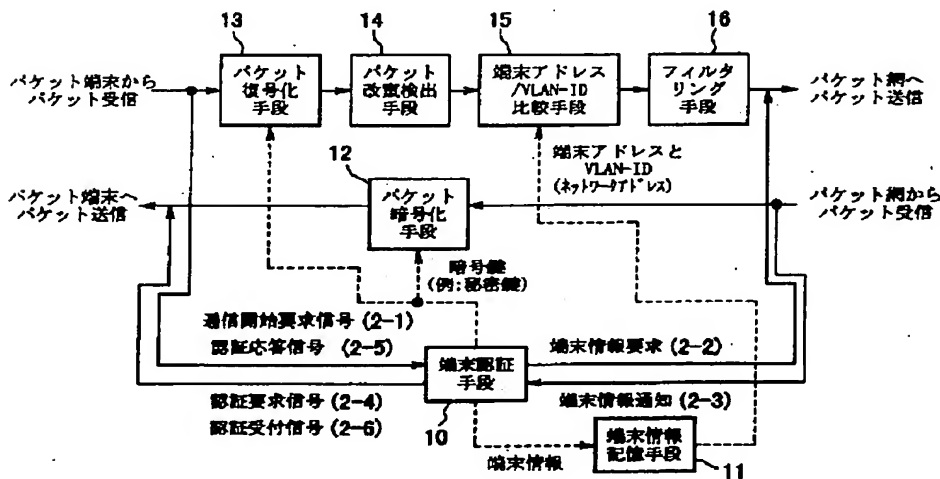
【図1】



【図5】

宛先 アドレス 4-1	送信元 アドレス 4-2	VLAN-ID 4-3	ユーザデータ (暗号化領域) 4-4
-------------------	--------------------	----------------	--------------------------

【図2】

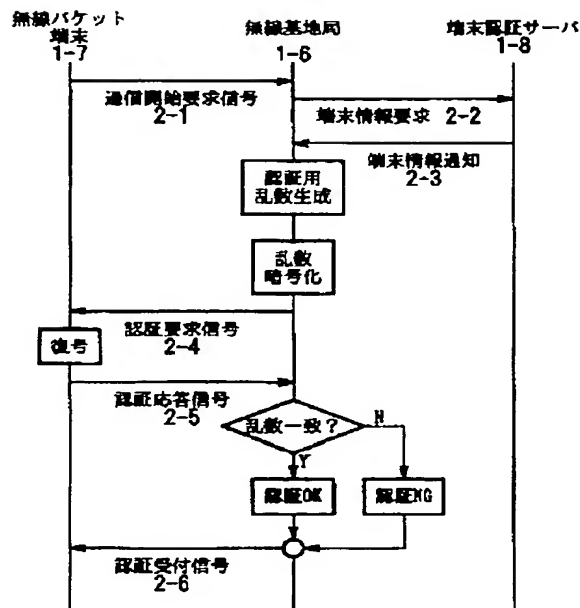


【図18】

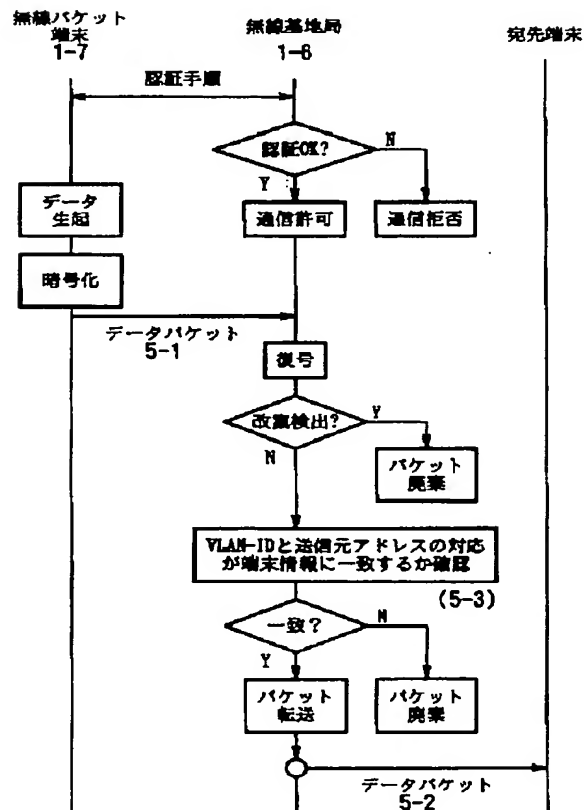
【図19】

ネットワークアドレス部	ホストアドレス部	宛先 アドレス 4-1	送信元 アドレス 4-2	ユーザデータ (暗号化領域) 4-4
-------------	----------	-------------------	--------------------	--------------------------

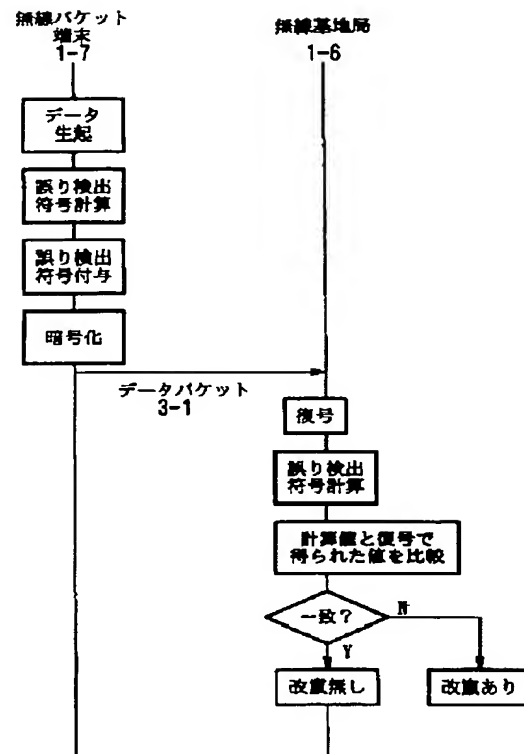
【 図 3 】



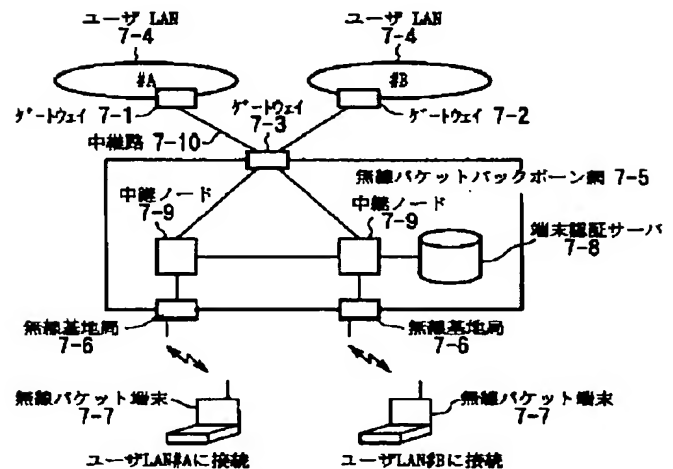
【 図 6 】



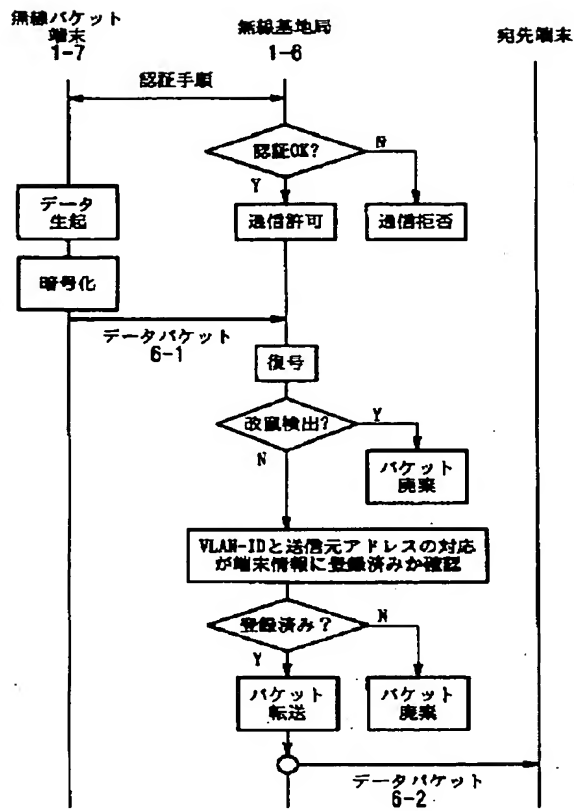
【 図 4 】



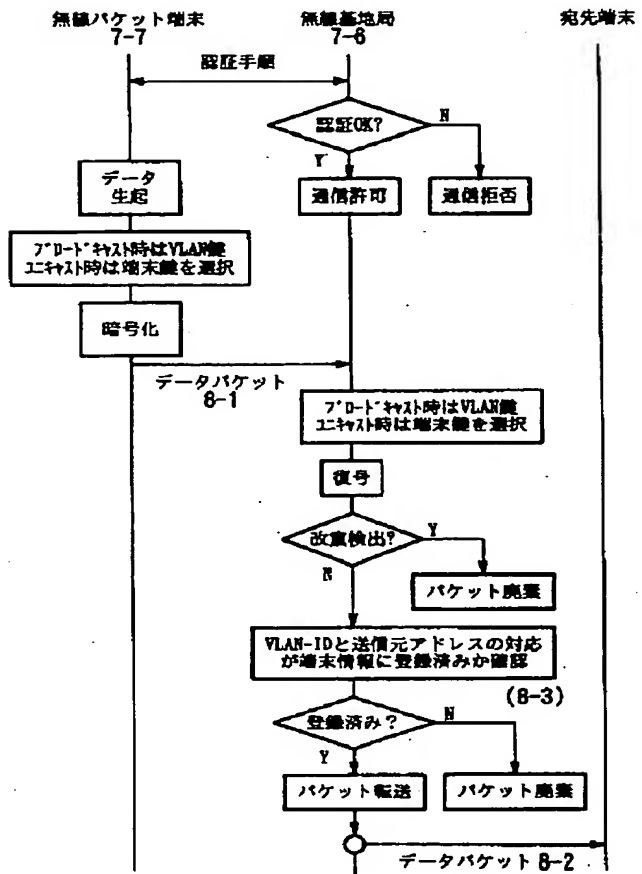
【 図 8 】



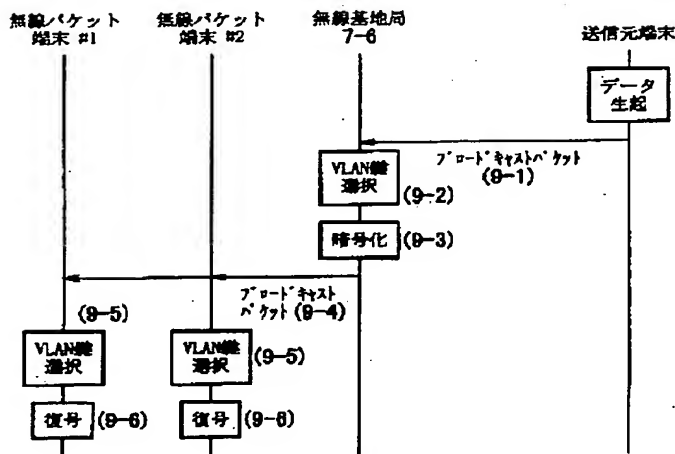
【図 7】



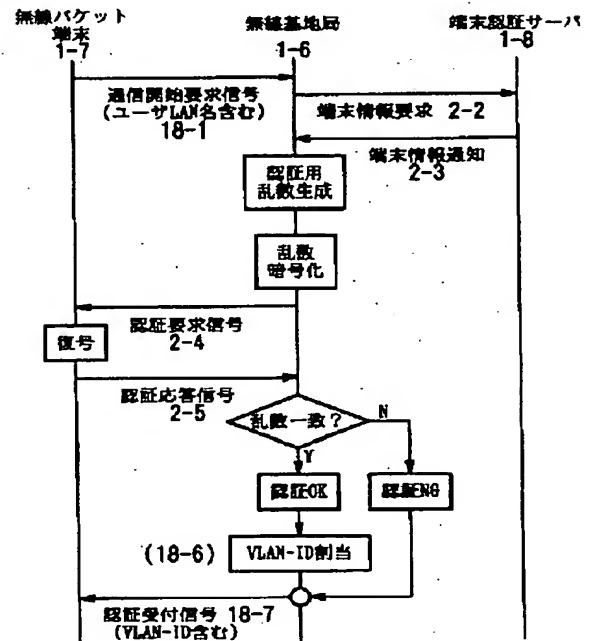
【図 9】



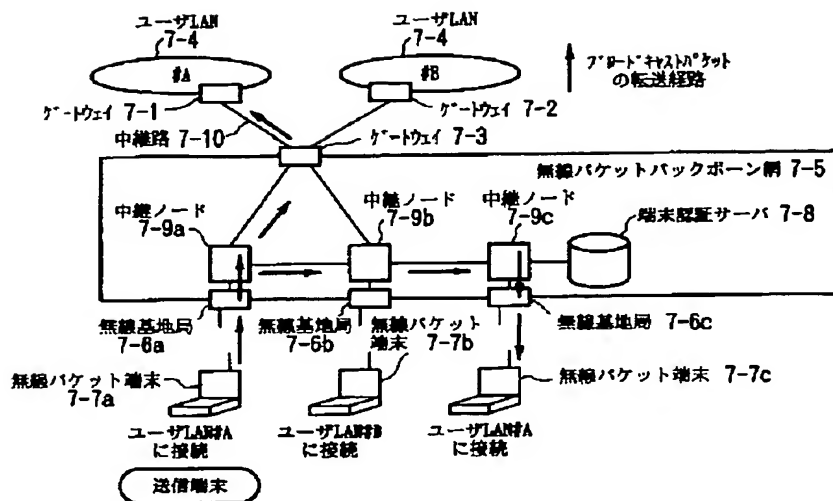
【図 10】



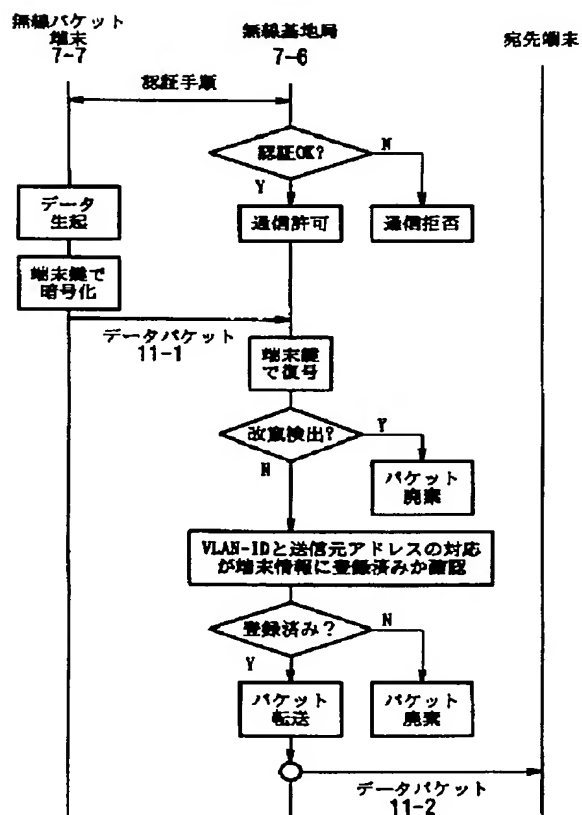
【図 14】



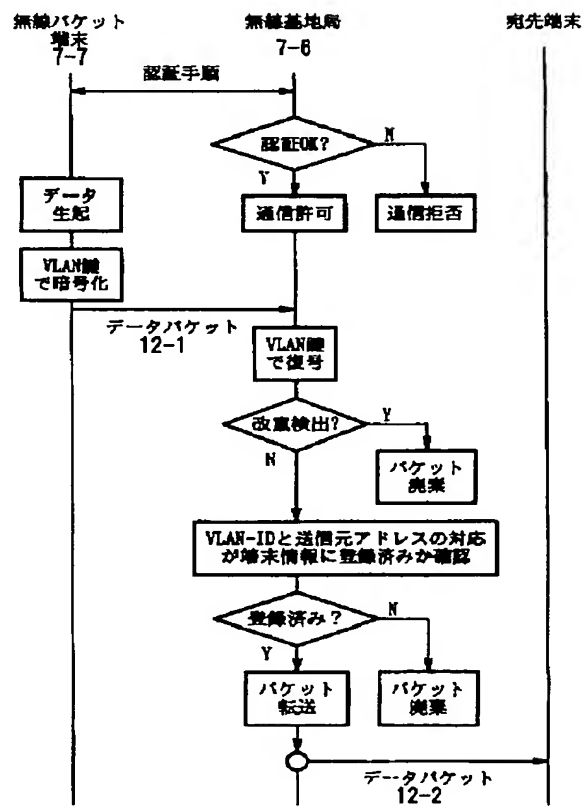
【 図 1 1 】



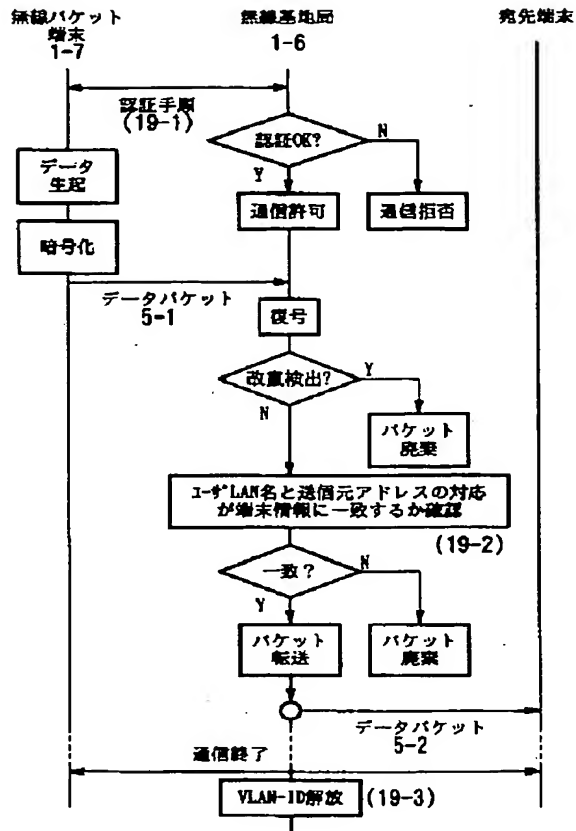
【 図 1 2 】



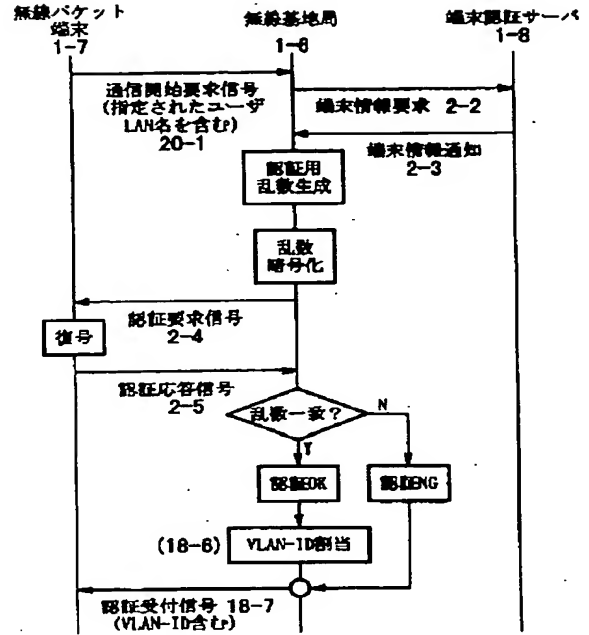
【 図 1 3 】



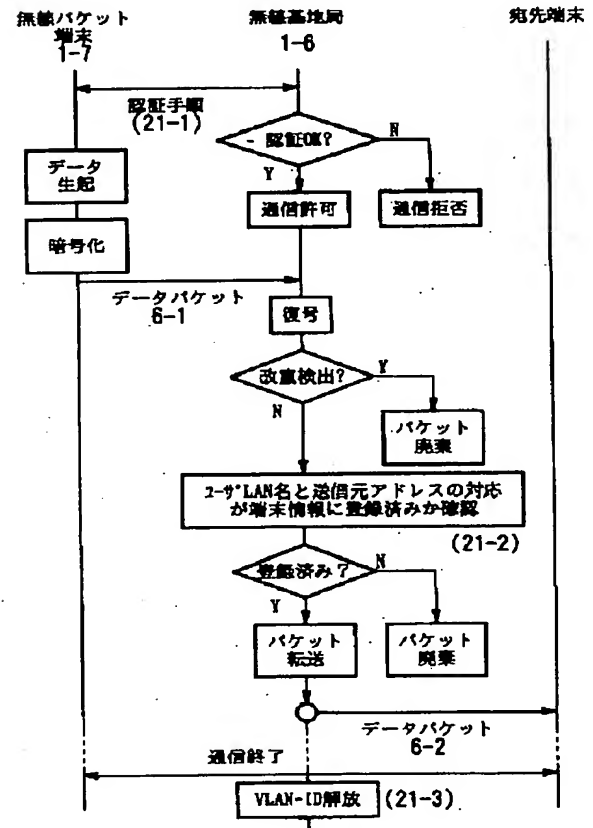
【図 1 5】



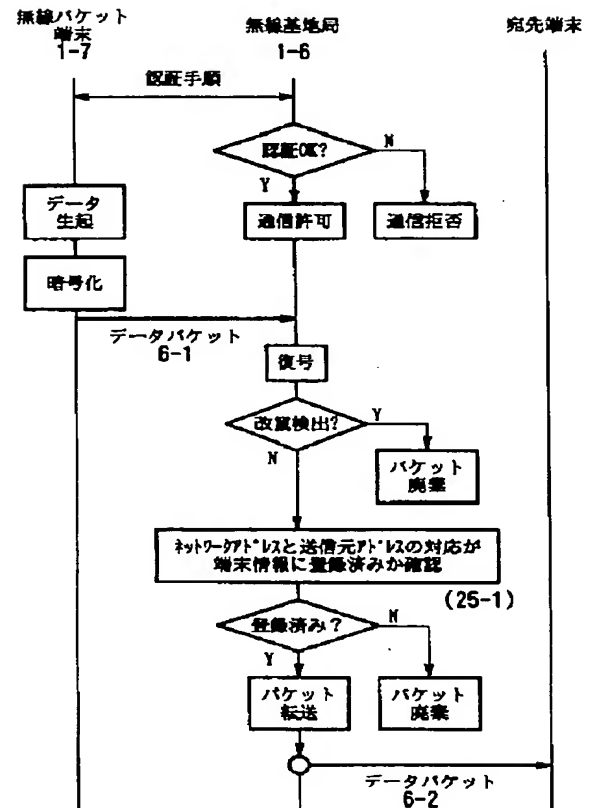
【図 1 6】



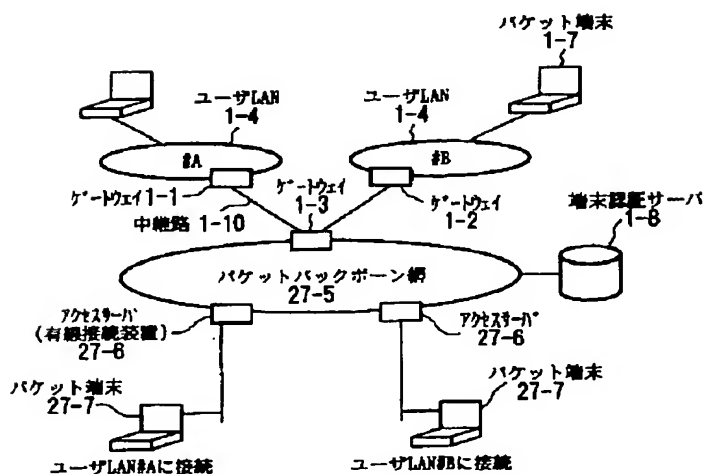
【図 1 7】



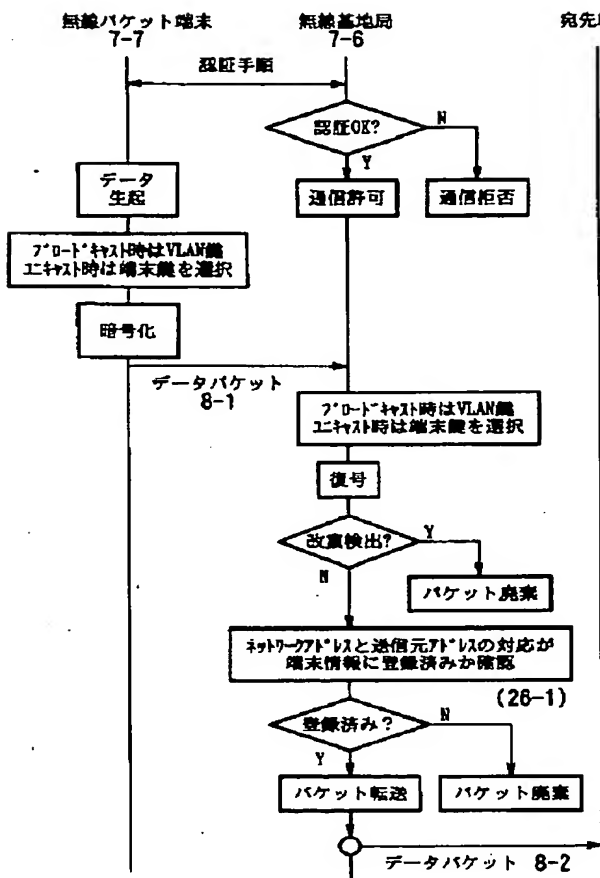
【 2 1 】



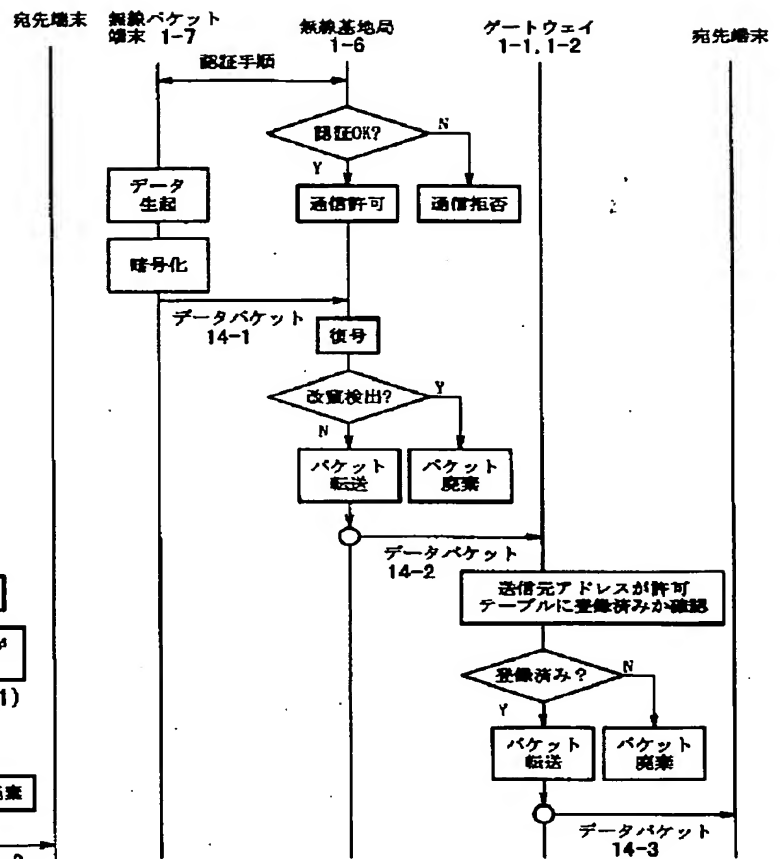
【 2 7 】



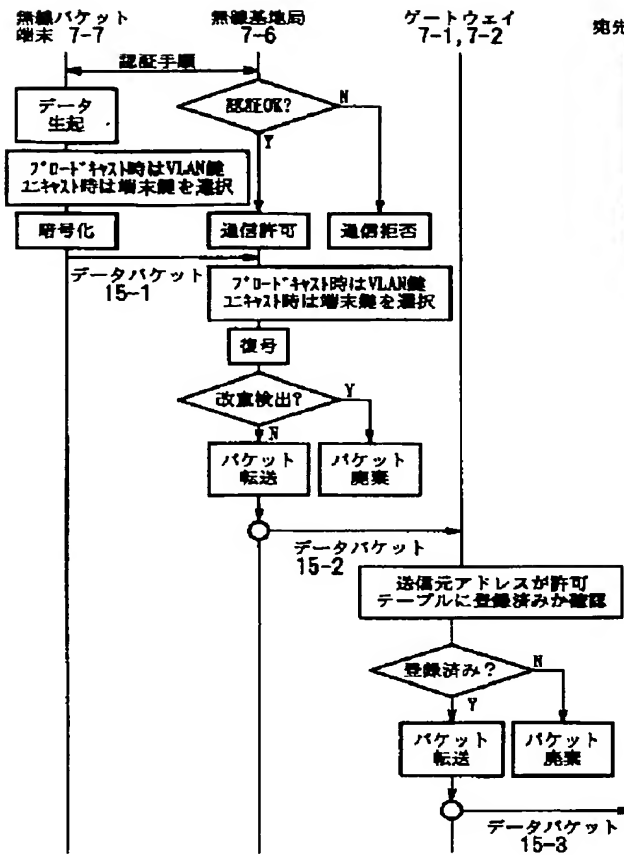
【図 2 2】



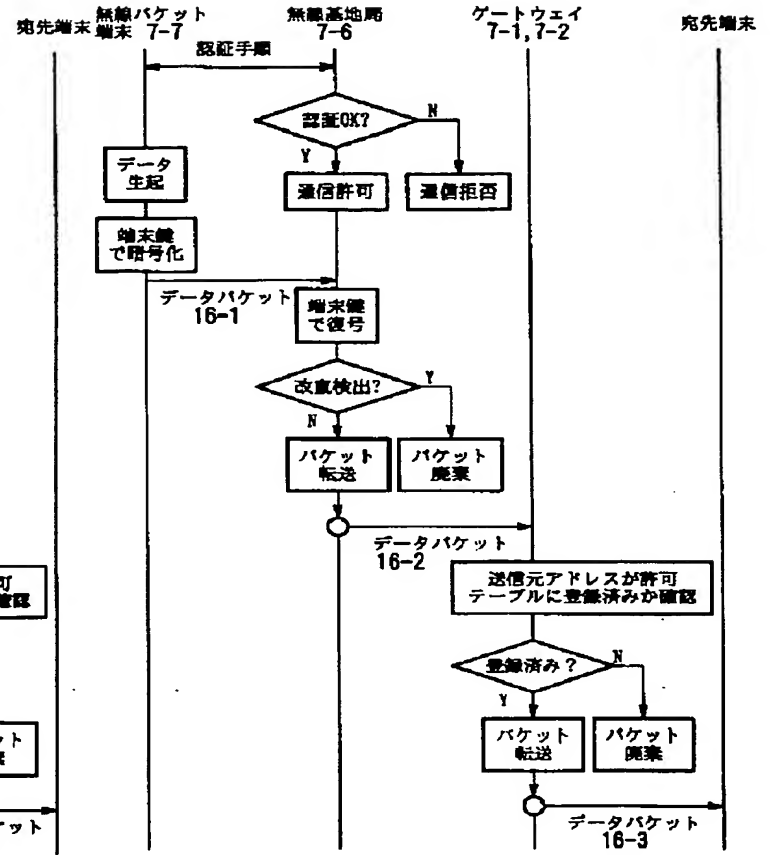
【図 2 3】



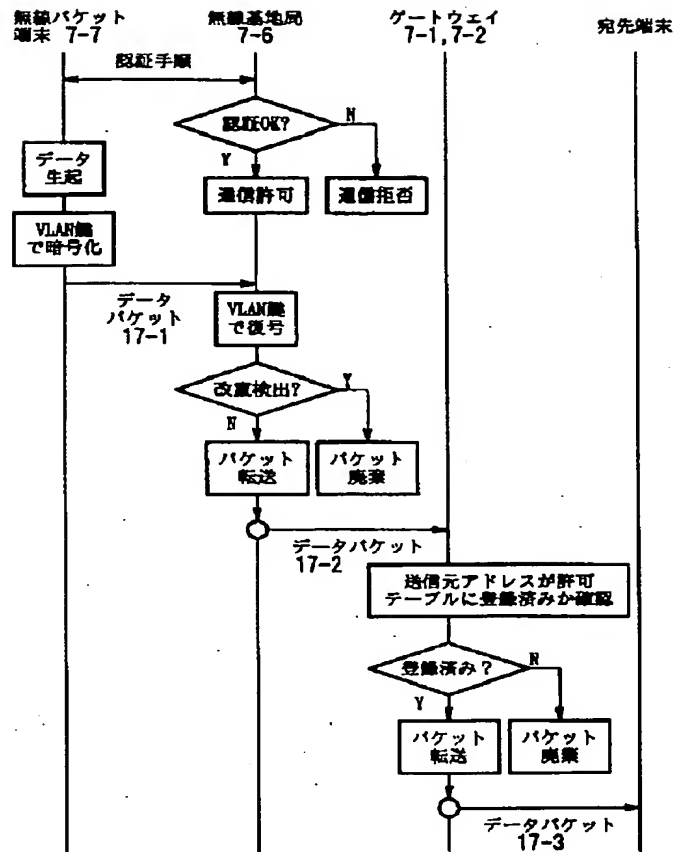
【 図 2 4 】



【 図 2 5 】



【 図 2 6 】



フロントページの続き

(51) Int. Cl.

12/66

12/56

識別記号

庁内整理番号

F I

技術表示箇所

673

C

11/20

B

102

Z

(72) 発明者 高梨 斉

東京都新宿区西新宿三丁目 19 番 2 号 日

本電信電話株式会社内

(72) 発明者 守倉 正博

東京都新宿区西新宿三丁目 19 番 2 号 日

本電信電話株式会社内

THIS PAGE BLANK (SP10)